Virginia Information Technologies Agency

VITA

2017 Commonwealth of Virginia Information Security Report

www.vita.virginia.gov

Prepared and Published by:
Virginia Information Technologies Agency
VITA - Powering the commowealth's digital government

Comments on the
2017 Commonwealth of Virginia Information Security Report
are welcome
Suggestions may be conveyed electronically to
CommonwealthSecurity@vita.virginia.gov

Please submit written correspondence to:

Chief Information Officer of the Commonwealth
Virginia Information Technologies Agency
Commonwealth Enterprise Solutions Center
11751 Meadowville Lane
Chester, VA 23836
cio@vita.virginia.gov

Virginia Information Technologies Agency

Contents

Executive Summary

This 2017 Commonwealth of Virginia (COV) Information Security Report is the tenth annual report by the chief information officer (CIO) of the commonwealth to the governor and the General Assembly. As directed by § 2.2-2009(B)(1) of the *Code of Virginia,* the CIO is required to identify annually those agencies that have not implemented acceptable policies, procedures and standards to control unauthorized uses, intrusions or other security threats. In accordance with § 2.2-2009(B)(1), the scope of this report is limited to the six independent and 72 executive branch agencies, including two Level I institutions of higher education. This report does not address compliance for Level II and Level III institutions statutorily exempted from compliance with Commonwealth policies and standards.

The CIO has established a commonwealth security and risk management (CSRM) directorate within the Virginia Information Technologies Agency (VITA) to fulfill his information security duties under §2.2-2009. CSRM is led by the commonwealth's chief information security officer (CISO).

This report has been prepared by CSRM on behalf of the CIO. It follows a baseline created by CSRM in 2008 to assess the strength of agency information technology (IT) security programs that have been established to protect commonwealth data and systems. A detailed listing of the agencies that were assessed and their security compliance and Cyber Security Framework assessment metrics are found in the appendices of this document.

CSRM supported VITA's information technology infrastructure services program (ITISP) offerings of agile and secure IT services for executive branch agencies. CSRM supported efforts to procure new IT security solutions and plan for transition from the commonwealth's current sourcing partner. CSRM worked with personnel from Department of Motor Vehicles, Department of Forestry, Department of Taxation, Department of Juvenile Justice, Department of Aging and Rehabilitative Services, Department of Education, Department of Accounts and Virginia 529 to create, review, and evaluate request for proposal (RFP) documents to procure IT security services for the commonwealth. VITA and agency personnel worked together to create a model that includes high quality security services offerings to protect the commonwealth from cyber threats, as well as satisfy the wants and needs of agencies throughout the commonwealth. The new security model when fully implemented will have increased encryption, cloud capabilities, identity and access management, and data loss prevention capabilities that will address previously identified risks. In addition, CSRM has been involved in the IT sourcing effort at VITA including the disentanglement process ensuring that controls are in place to protect the confidentiality, integrity and availability of commonwealth information assets.

CSRM proposed updates to the Hosted Environment Information Security Standard and the IT Information Security Standard.

Proposed standard changes are reviewed by a policy committee comprised of agency information security officers. In addition, stakeholders can review the changes on the public Online Review and Comment Application (ORCA) site and provide feedback to commonwealth security on the proposed requirements. Commonwealth standards will be revised as necessary to provide effective governance for commonwealth's environment. CSRM recommends that agencies actively engage in the policy review and comment process to facilitate relevant and effective IT security standards for the commonwealth.

VITA's centralized services offer support to improve agency security programs and enhance information security.

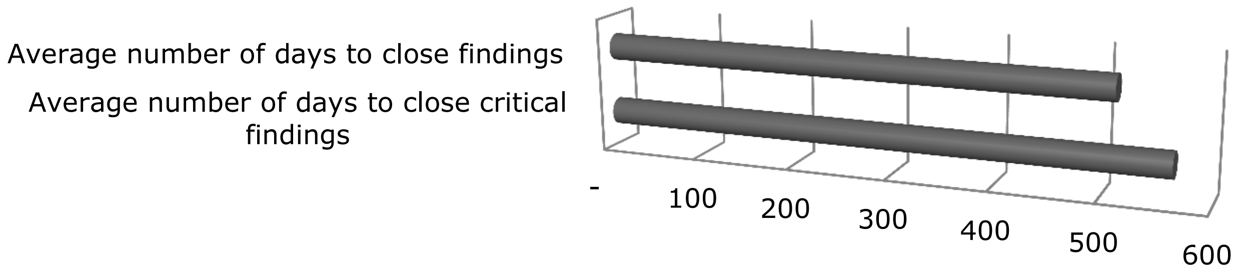
IT security audit services, information security officer (ISO) services, and vulnerability scanning services work together to promote information security in the commonwealth. These services assist agencies in evaluating their IT security programs effectiveness and complying with commonwealth IT security requirements. There are 29 signed audit services clients in 2017 for the audit services, an increase of six clients from the prior year. For the agencies using this service, the percentage of sensitive systems that have been audited increased by 22 percent from 2015 to 2017 and we anticipate nearly all audits of the audits of these sensitive systems will be completed by 2020. There are 31 agencies participating in the centralized ISO service. This is also an increase of six agencies from the prior year. For these agencies, the percentage of risk assessments completed for sensitive systems has increased by 26 percent from 2015 to 2017. We anticipate nearly all of the risk assessments for sensitive systems will be done by 2020. Lastly, the vulnerability scanning service assisted 77 agencies and performed more than 1,300 vulnerability scans each quarter of public-facing websites in 2017 to assess the commonwealth's security posture. Agencies also worked to reduce their footprint even more than last year by decommissioning legacy applications and moving sites behind the secure perimeter. The centralized security services complement each other to identify risks to commonwealth information and develop action plans to further safeguard the commonwealth's information assets. Agencies participating in the centralized services should continue their work with CSRM personnel to continue to bolster the agencies' information security programs.

The commonwealth was a target of ransomware attacks.

In these attacks the sender poses as a trustworthy source and uses fraudulent emails or links to malicious websites to load software designed to block a victim's access to their computer, essentially holding the user's data hostage until a ransom is paid to the attacker. The incident response team offers simulated phishing campaigns to agencies to allow agencies to incorporate social engineering training as part of their security awareness training programs and five agencies took advantage of this program in 2017. Each campaign was tailored to the specific agency and their mission. The simulated phishing campaign results this year indicated a 50 percent decrease in the number of employees that gave away their credentials, indicating that the simulated phishing campaigns are an effective method of providing additional security awareness training. CSRM plans to continue this service to agencies upon request. CSRM has also contributed to the design of security controls in the future messaging service to further combat ransomware and other phishing attacks. CSRM recommends that agencies continue to provide practical and effective security awareness training, as well as implement two-factor authentication to reduce the impact of these social engineering attacks.

Agencies are not remediating findings timely, leaving agencies vulnerable. Agencies reported that they closed 441, or 14 percent of open findings in 2017. These findings were open an average of 512 days, taking more than a year to remediate and close information security issues that have been identified. In addition, it took agencies an average of 565 days, seven weeks longer to close findings associated with critical controls. We consider critical controls to be those associated with the Center for Internet Security (CIS) Controls. Such controls have been identified as best practices to protect organizations from known cyberattack vectors. CSRM will investigate new methods to report outstanding and overdue findings to further encourage agencies to remediate critical findings quickly. We recommend that agencies dedicate the appropriate resources to remediate their findings timely. Agencies should prioritize and remediate findings by criticality, first addressing the findings that area associated with critical controls.

Days to Close Audit Findings



Commonwealth security works with the VITA IT strategic planning process to help ensure agency security needs are addressed as agencies develop their strategic planning.
CSRM considers the adequacy of an agency's information security program when reviewing its strategic plans to determine if agency resources have been allocated to resolve existing security issues prior to investing in new technologies. If agency compliance metrics indicate there are existing security issues that should be resolved before the agency invests in new technology, CSRM will work with the agency to help ensure agency security needs are addressed before new technology investments are made. CSRM recommends that agencies address outstanding operational risks/issues (ORIs), such as end-of-life systems, significant weaknesses in IT security audit programs, or deficient risk management programs, promptly to enhance overall agency security and expedite the CSRM review of the agencies' strategic plans.

Threat analysis will change with the move to a new multi-supplier environment. The addition of new vendors and new security tools will provide enhanced capabilities to analyze and monitor threats to commonwealth security. Agencies will have additional monitoring tools and a more in depth view into their environment. Agencies will need to be engaged with VITA and the new vendors to fully implement the new tools and take advantage of these opportunities afforded by the new technologies.

Agency audit program compliance metrics improve.
Agency submissions of completed IT security audit plans and IT security audit reports improved in 2017, which contributed to the six percent increase in overall audit program compliance. Key contributors to the improving audit compliance metrics are the additional resources that were made available for agencies to procure IT security audits and the audit work completed by VITA centralized audit services. Centralized audit services completed IT security audits for 123 sensitive applications in 2017. In addition, the centralized audit services submitted IT security audit plans and facilitated IT security corrective action plans for customer agencies. These audits are important as they help agencies identify potential weaknesses in the design or effectiveness of their IT security controls so that the issues can be addressed before they are exploited by malicious actors. CSRM noted that there are 20 agencies with audit compliance grades of D or F that were not signed up for the centralized audit services. While these agencies must develop a plan to address their lack of IT security audit plans and audits, CSRM is also investigating additional measures to help ensure that these necessary IT security audits are performed. CSRM anticipates IT security audit compliance metrics will continue to improve as centralized audit services becomes fully staffed and continues to complete IT security audits.

Institutions of higher education continue to be frequent targets of cyberattack.
Based on the analysis of Multi-State Information Sharing and Analysis Center (MS-ISAC) security investigations in 2017, higher education has the most investigations, with more investigations than the total number of local government, public education and state government investigations combined. These institutions are seen as attractive targets by attackers due to the significant amount of sensitive information that they manage, which can include personal identifiable information (PII), medical health records, law enforcement, and intellectual property information. To address these issues, CSRM recommends that a work group is convened to study the effectiveness of the current IT governance practices in higher education, which have allowed several institutions to be exempt from any external IT security oversight. The work group can develop recommendations to address the persistent security threats facing these institutions, including considering the establishment of one IT governance oversight body for all of higher education that would establish consistent IT security requirements, monitor compliance, and ensure that appropriate corrective actions were taken.

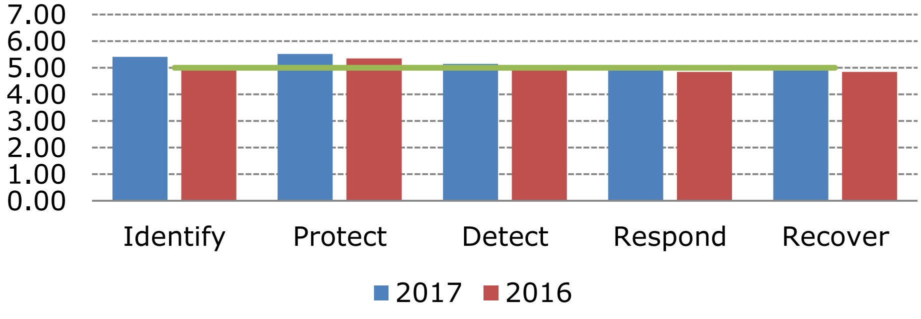
Agency risk program compliance improved by five percent.
Risk program compliance analysis shows that 41 percent of agencies have implemented a comprehensive risk management program, an improvement from the prior year. The risk program metrics are based on an evaluation of agency risk assessment plans, risk assessments, business impact analysis, data set analysis, and ISO certification. Centralized ISO services are committed to assisting 31 agencies develop effective risk management programs. In addition, agency personnel are working to prioritize risk management in the commonwealth as a necessary part of an effective agency IT security program. CSRM determined that 89 percent of agencies with poor risk compliance metrics (grades of D or F) did not take advantage of the centralized ISO service offerings that

could have supported their risk management efforts. These agencies are required to provide a plan to address their risk management program deficiencies. CSRM is also exploring new means to further support agencies' risk management efforts. Overall, CSRM anticipates that risk management program compliance metrics will continue to grow as agencies dedicate the necessary resources to address this issue.

The commonwealth participated in the Nationwide Cyber Security Review (NCSR), a self-assessment survey aligned with in the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) to evaluate the commonwealth's cybersecurity posture and compare with other states. The results are summarized by the core elements of the NIST cybersecurity framework, which are the following basic cybersecurity functions: identify, protect, detect, respond and recover. Survey results indicated that agencies on average have partially documented standards and/or procedures in all five cybersecurity functions. Agencies reported that their processes were least mature in the "recover" function, where agencies need to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity event. The "protect" function, related to agencies' ability to limit or contain the impact of a potential cybersecurity event, is where agencies indicated their processes were the most mature. Agencies should use the survey results to prioritize their IT security efforts, as well as a benchmark to gauge progress in the maturity of their cybersecurity posture and assisting in cybersecurity investment decisions. Agencies should strive toward optimized maturity where each organization has policies, standards and/or procedures to achieve their objectives, and implementation is not only tested and verified but also regularly reviewed, improved and repeated to ensure continued effectiveness of their controls.

The average score for each function improved in 2017 from the prior year. According to NCSR, the recommended minimum maturity level is set at a score of five and higher and the agencies reported that they reached this level for nearly every function on average.

CSF Framework
Averages by Function
2016-2017



2017 Annual Information Security Report

The 2017 Annual Security Report for the Commonwealth of Virginia report includes an analysis of the commonwealth threat management program, new services offered, the commonwealth information security governance program and the commonwealth risk management program.

Commonwealth Threat Management Program

The threat management program monitors and manages potential malicious IT attacks against commonwealth agencies and information. CSRM collects information from within the VITA IT infrastructure program, as well as agencies falling outside the scope of the IT infrastructure program to evaluate the commonwealth's threat posture overall. This information is analyzed to identify threats affecting the commonwealth, to identify widespread vulnerabilities, and to respond appropriately. Some of the key components of the program are highlighted in this report.

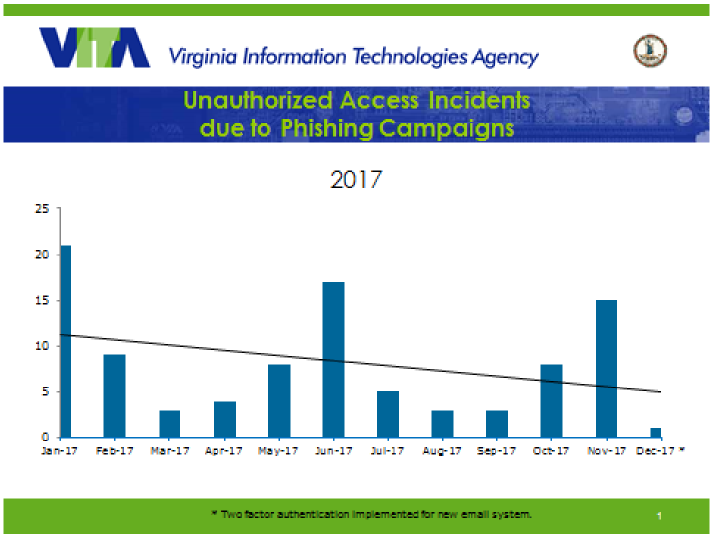
Commonwealth Cyber Threat and Attack Analysis

The *Code of Virginia*, *§2.2-603(F)*, requires all executive branch agency directors to report IT security incidents to the CIO within 24 hours of discovery in accordance with security standard SEC501-09. The CSIRT then categorizes each security incident based on the type of activity.

During 2017, the Commonwealth of Virginia continued to be a target for cyberattack.
The commonwealth experienced 47 million attack attempts on the network and blocked 567 million pieces of spam and more than 781,000 pieces of malware. Despite many layers of protection, the commonwealth still experienced 323 successful IT security incidents.

Social engineering remains the primary attack vector for initial access to the commonwealth environment.

Commonwealth of Virginia employees are a constant target for social engineering attacks. These attacks take multiple forms. Some are conducted as phishing attacks seeking to harvest user credentials, others are malicious attachments posing as invoices or order receipts and some are even popups informing the user that their device has been infected and they should call a toll-free number for assistance.


Virginia Information Technologies Agency

Unauthorized Access Incidents
due to Phishing Campaigns

* Two factor authentication implemented for new email system.

1

Phishing attacks were the number one source of unauthorized access to COV systems. In 2017, the commonwealth experienced 143 unauthorized access incidents. Of these incidents, 97 (68 percent) were due to employees responding to a phishing message and the attacker using these credentials. In early December 2017, CSRM piloted two-factor authentication for the new email system. This control prevents the attacker from remotely using the compromised credentials to access the COV email system. The results of the pilot show that there was a 93 percent decrease in this type of incident during the first month of implementation (December 2017). Using this data, we project we should see a 30 percent overall decrease in total incidents for 2018.

Malware incidents remain a serious threat to commonwealth systems. As the second largest category of incidents, malware is a constant threat to commonwealth devices and data. Malware programs are designed to infect legitimate users' computers to damage systems or provide unauthorized access to sensitive data.

During 2017, the volume of malware incidents rose 17 percent from 2016. As the commonwealth employs a defense in depth approach, attackers found that it was more effective to deliver emails with malicious attachments to users than to directly attack COV systems. Users would open the malicious attachments believing it was legitimate business documents from vendors inadvertently infecting their devices with malware.

In April 2017, this technique was used as the infection vector for a malware incident at one of the COV agencies. A user opened a malicious attachment thinking it was a legitimate invoice and succeeded resulting in the infection of a system. The malware spread to other systems on the network using administrative rights, misconfigurations, end of life software and missing patches.

In response to this attack vector, CSRM developed a new control that can detect this type of attack and prevent the arbitrary code from executing on COV devices. Following the implementation of this new control, the number of malware incidents decreased.

In December 2017 there was another spike in malware incidents. With the deployment of Google Chrome to the email pilot users, the hardening standard allowed for users to install browser extensions. As a result of these installations, an unauthorized software called Coin Miner was found in the users' Google cache.

Coin Miner is a cryptocurrency mining application that utilizes system resources to mine virtual currencies such as Bitcoin or Monero. These cryptocurrencies can be used for legitimate purposes and are recognized by some countries as legitimate currency. However, cryptocurrency can also be used by cybercriminals to support their criminal activities. While some users may intentionally install crypto mining software on their systems, it is often installed without their knowledge, typically resulting in performance issues. The COV installations were not authorized and were removed once discovered.

The appearance of Coin Miner in the environment alerted CSRM to the fact that the hardening standard for Google Chrome needed to be adjusted. CSRM developed a list of approved extensions for the commonwealth to utilize. Any extensions that are required for legitimate business purposes that are not on the approved list will be handled through the security exception process.

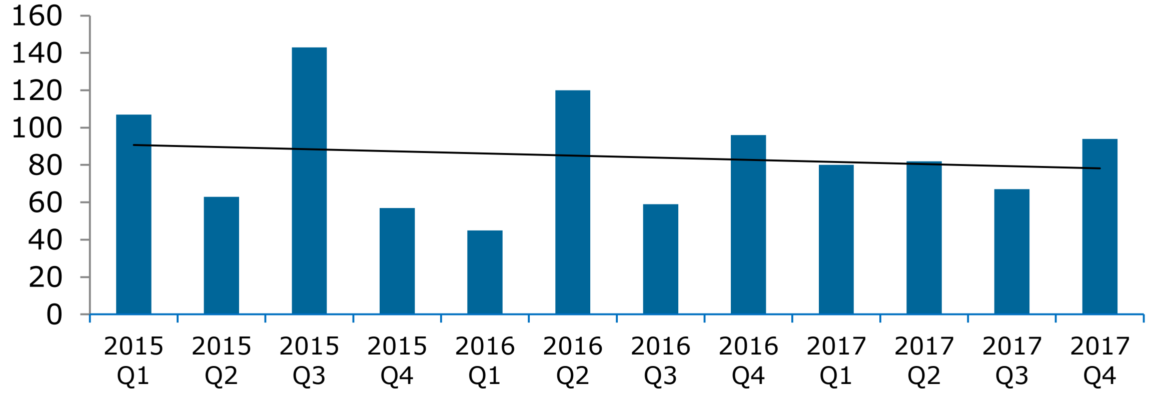
Security awareness training is key to protecting COV employees, systems and data from cyberattacks.

As the attack landscape is constantly changing, the primary point of defense remains the same – the employee. While technical controls can be put in place to protect the environment, the only effective approach is employee training. The COV IT Security Standard (SEC501-09) requires all employees to take security awareness training annually; this allows a large amount of time between training for attackers to develop new techniques and employees to forget what they have learned. In order to supplement this yearly training, CSRM has developed a free service where agencies can request simulated phishing campaigns to reinforce the security awareness training and to allow users to practice their skills in a safe environment.

During 2017, CSRM performed simulated phishing campaigns at five agencies as part of their security awareness training programs. These simulated phishing campaigns were developed on for each agency to be relevant to that agency's business needs. Campaigns were run for several days and detailed reports were provided to agency ISOs at the end of the campaign. Of the 6,038 employees that were targeted, 1,213 employees (20 percent) opened the email. Of those employees who opened the emails, 406 (33 percent) who opened the email clicked on the link inside the email and 215 (53 percent) of those employees who clicked the link ultimately provided credentials. The simulated phishing results in 2017 indicated a 50 percent decrease in the number of employees that gave up credentials. The percentage for 2017 of users submitting their credentials to a phishing campaign decreased from eight to four percent, indicating that the simulated phishing campaigns are an effective method of providing additional security awareness training.

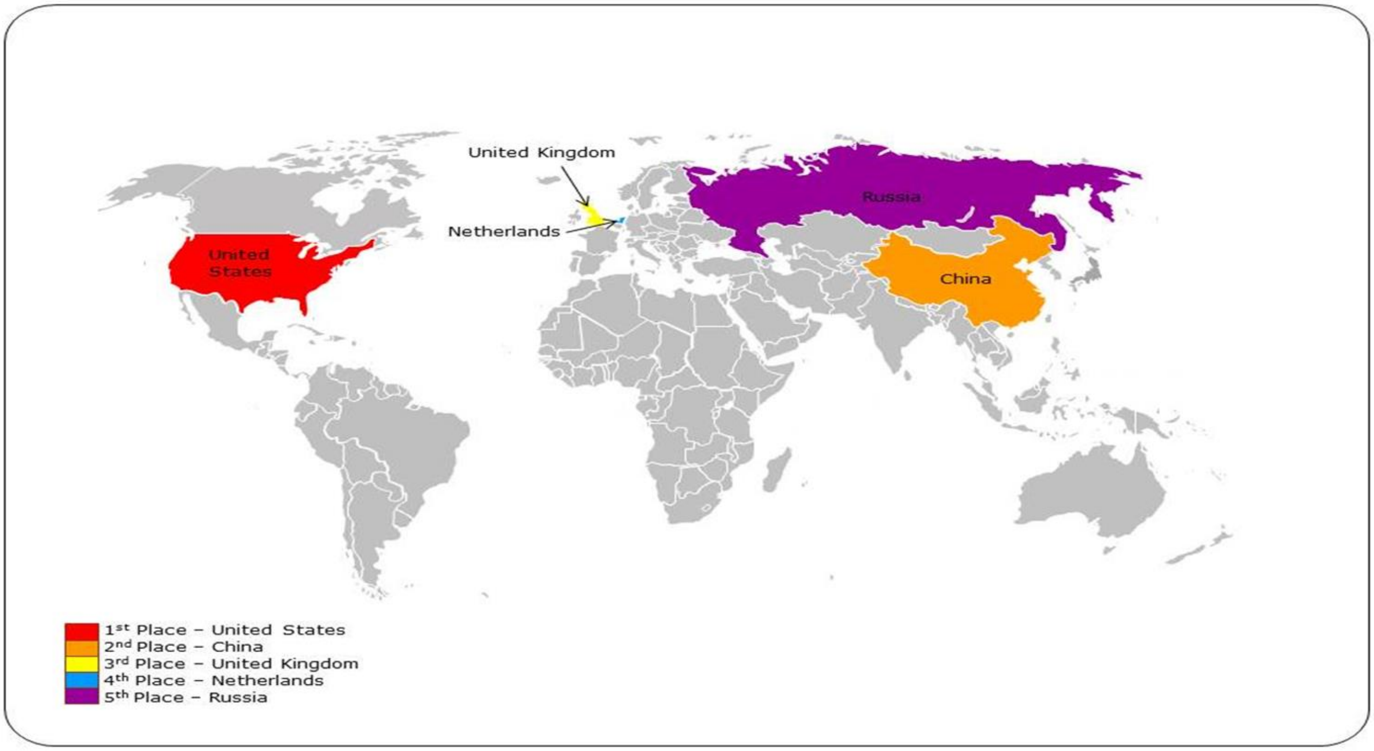
Cybersecurity incident trends continue to be monitored.
CSRM has been working diligently to protect commonwealth systems from cyber threats. As best practices are implemented and additional layers of protection are added, attackers develop new tactics to compromise systems. CSRM is continually investigating new security controls to protect the environment from compromise. In January, May and November of 2017, the commonwealth experienced on-going phishing campaigns resulting in the number of incident being higher than the previous year for those quarters. In addition, the Coin Miner malware infections detected after the Google Chrome deployment resulted in the fourth quarter experiencing the largest number of cyberattacks for the year.

Incident Trends
2015 – 2017



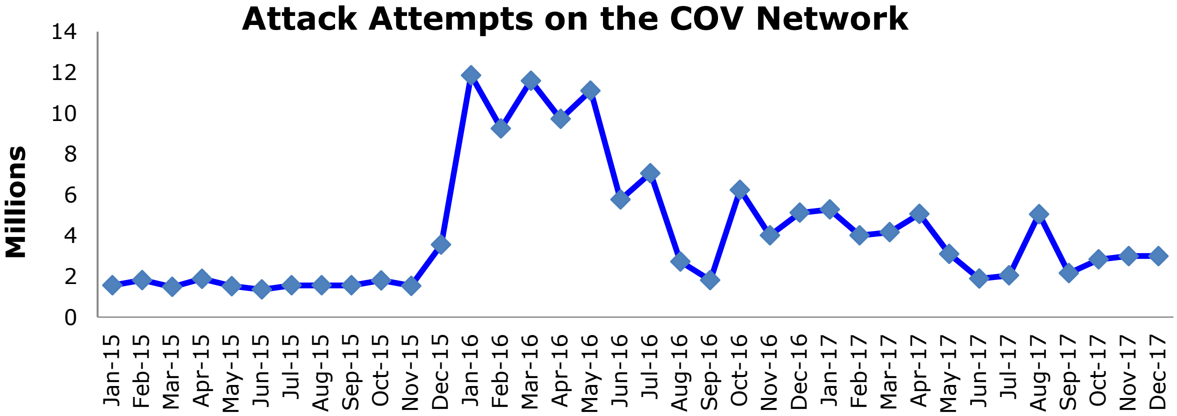
The origins of the attacks on the commonwealth's network are monitored and tracked.
CSRM receives threat intelligence information from multiple sources. This information is incorporated into the security monitoring systems that protect the commonwealth's data from

attack. In correlating this information with our intelligences partners we are able to proactively block origins of attack before systems are compromised. During the past year, this information indicated that the top five countries where attacks against the commonwealth originated were the United States, China, United Kingdom, Netherlands and Russia. As the attack attempts may be coming from hacktivist groups or state sponsored actors, attackers consider the data housed in the commonwealth's IT assets to be a valuable resource in the global marketplace. CSRM will continue to monitor the origins of these attacks and respond promptly to attacks on our networks, regardless of their origin.



Attack attempts

During 2017, over 41 million attack attempts were detected against commonwealth systems. This is a rate of one attack every 1.32 seconds. As new attack types are discovered, systems are tuned to block them. In addition, as normal COV traffic is identified, systems are adjusted to prevent false positives. Each spike in traffic is indicative of a new type of traffic that is being seen. The drop following the spike is due to the tuning of the systems. This is evident in the drop in attack traffic during May and June 2017, when systems were being actively tuned to address the changing threat landscape.

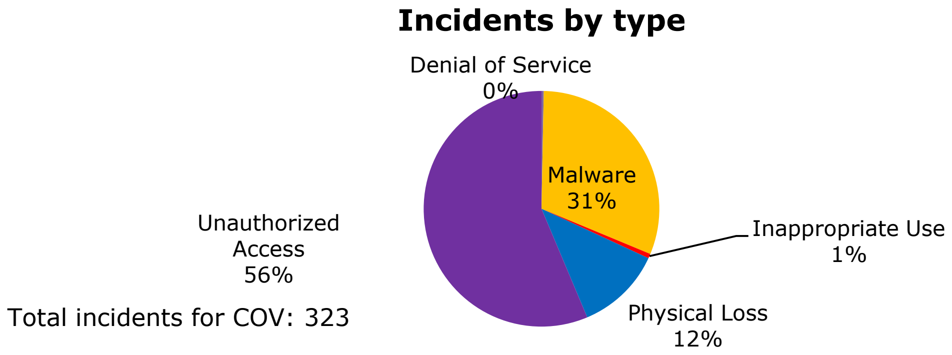


Incident trends by category

Reported security incidents are analyzed and grouped into one of the following categories described below:

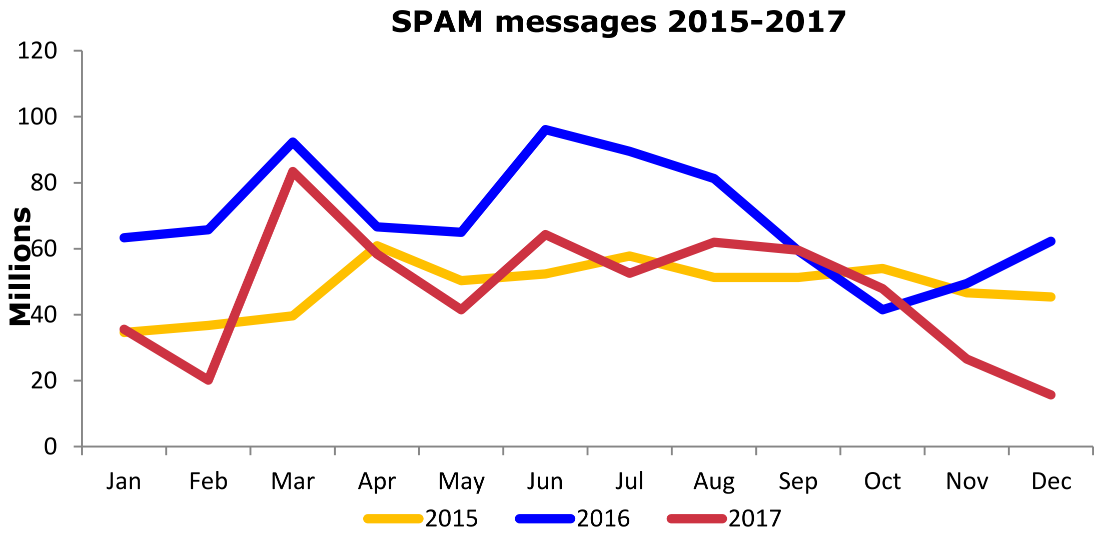
- Denial of service - Loss of availability of a COV service due to malicious activity
- Inappropriate usage - Misuse of COV resources
- Malware - Execution of malicious code such as viruses, Trojans, ransomware, spyware and key loggers
- Phishing - Theft or attempted theft of user information, such as account credentials
- Physical loss - Loss or theft of any COV resource that contains COV data
- Unauthorized access - Unauthorized access to COV data

During 2017, unauthorized access to COV data became the top category for security incidents. Attackers used social engineering attacks and phishing campaigns to harvest user credentials and to gain unauthorized access to COV systems. Malware dropped to second place with physical theft/loss moving into third. Security awareness training, implementation of multifactor authentication, and full disk encryption are controls VITA has implemented to limit the impact of those incident categories. Teaching users to protect their passwords and to utilize unique passwords for each account sign-on instance help reduce the likelihood of such incidents. Full disk encryption is leveraged to mitigate data loss in hardware thefts; however, as this issue is also attributed to user behavior, theft prevention is also included in security awareness training.



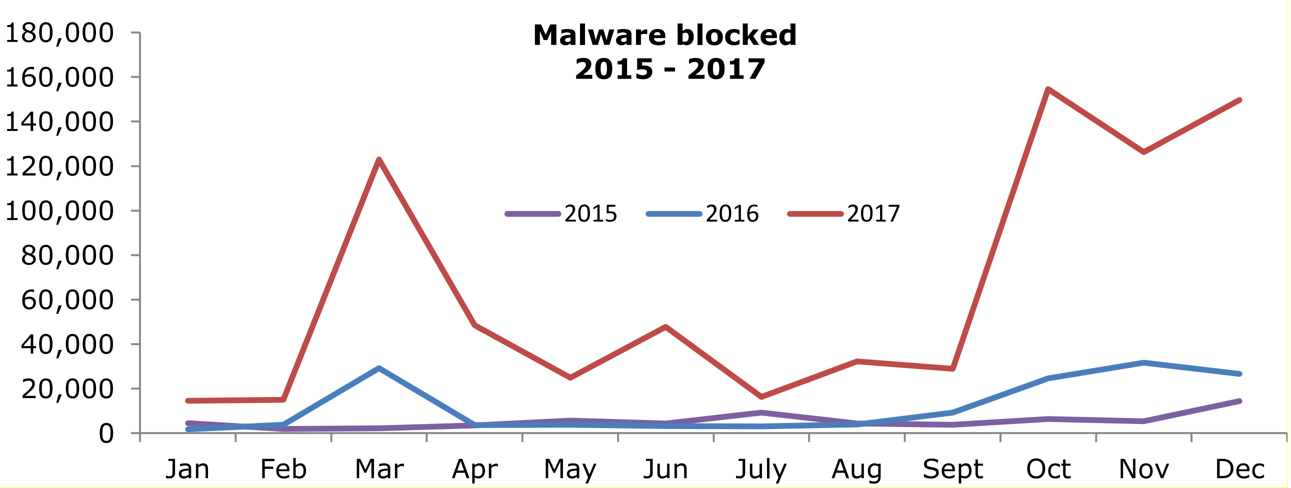
SPAM messages

Email is an important part of the commonwealth’s communication and is highly utilized in the course of daily business. Effective security tools must be in place to minimize malicious email activity in the enterprise environment to protect commonwealth information assets. In 2017, the commonwealth filtered more than 567 million spam messages, 87 percent of all email received. This is a 32 percent decrease from the prior year. Going forward with the new email system, CSRM will not be able to provide this information as Google does not break out these statistics by customer.



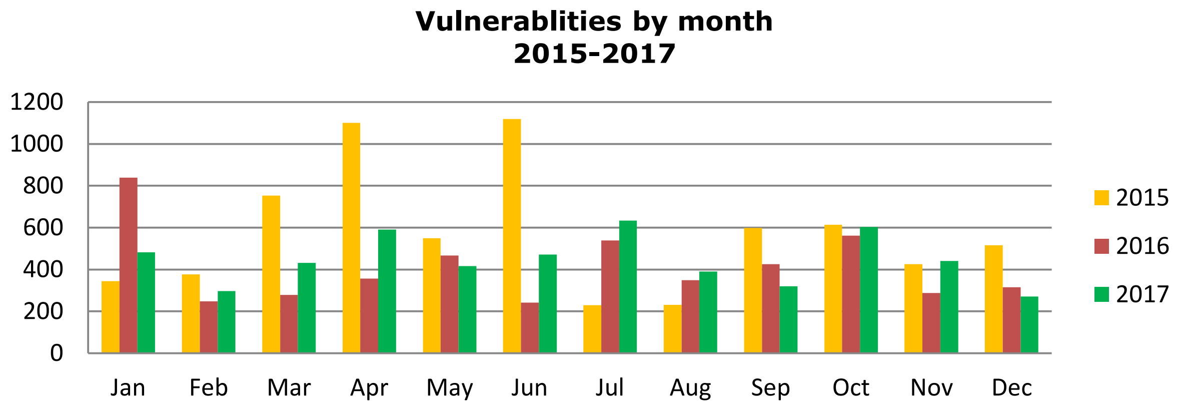
Malware blocked

During 2017 the commonwealth experienced a 440 percent increase in the number of malware attempts blocked from reaching COV systems. During the year several large malicious spam and advertising campaigns were blocked by the McAfee Web Gateways, causing the increase in number of pieces of malware blocked. These campaigns were detected as utilizing JavaScript and Flash exploits to attempt to infect COV devices. While 781,453 pieces of malware were blocked, the commonwealth experienced 100 successful malware infections, an increase of 20 percent from 2016. Of the malware incidents that were experienced 79 percent were due to malicious content being delivered to the device via email. The remaining 21 percent of incidents was the result of Coin Miner malware impacting the Chrome browser.



Vulnerability tracking

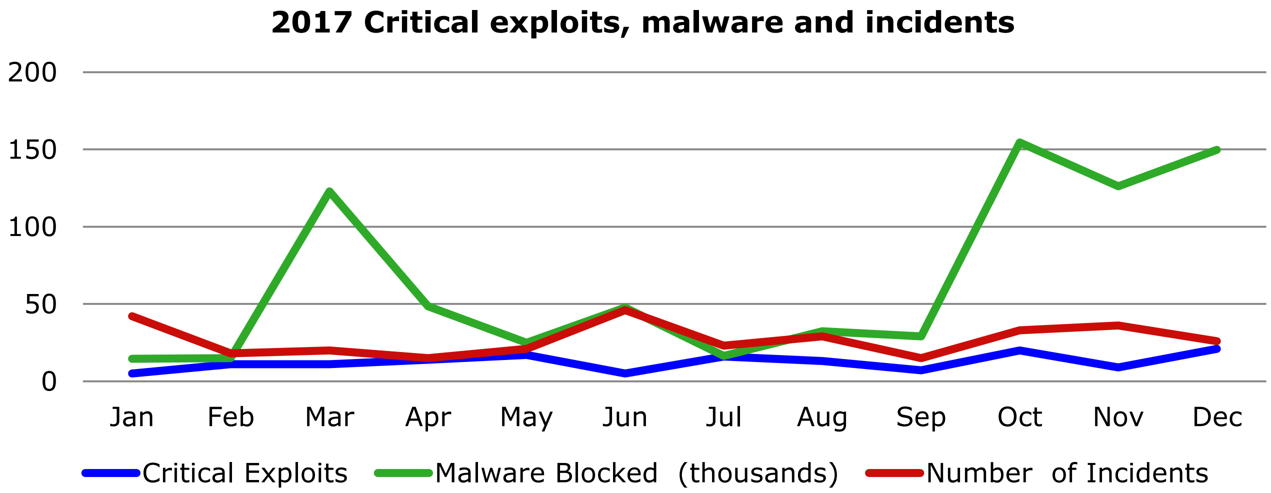
As part of tracking threats to the commonwealth, CSRM monitors COV systems for newly discovered vulnerabilities and incorporates them into a weekly advisory. This advisory is distributed to localities, state agencies and higher education. In 2017 the advisory identified 5,345 vulnerabilities that could affect commonwealth systems. ISOs can use this information to ensure that systems are being patched in compliance with security standards.



Critical exploits decreased slightly from the previous year

Zero-day vulnerabilities are newly discovered vulnerabilities that do not have patches available. These vulnerabilities are prime targets for attackers. Attackers develop exploit code using these vulnerabilities to install malware on a device before the vendor can provide an update or patches can be applied. As attackers publish the exploit code in the wild, these zero-day vulnerabilities pose an increased risk to the environment.

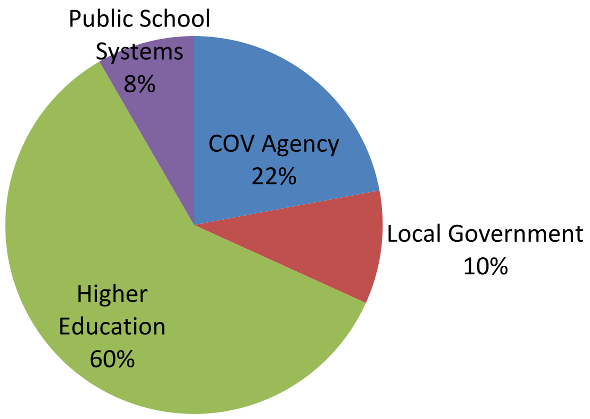
During 2017, the total number of critical exploits decreased slightly, from 132 to 125, a five percent decrease. However, as summarized on the chart below, critical exploits have a direct correlation to the amount of malware that is blocked and the number of incidents that occur. As malware remains the second largest category for incidents, it is important that critical exploits are patched as soon as possible after appropriate testing.



Cyber Intelligence from Commonwealth Partners

The information received from commonwealth partners includes data involving state and local governments, higher education and public schools systems. The majority of the data is reported by MS-ISAC as potential events that they have monitored on the internet. CSRM disseminates the alerts to the affected entities and tracks them as investigations, since the results of the alert are unknown. In 2017, the commonwealth completed 243 investigations for the 2,526 alerts that were received. This was a 26 percent decrease from 2016. The following chart shows the percentage of investigations by type of entity.

2017 Percentage of investigations



Cyberattacks and other incidents at Virginia colleges and universities remain a significant risk.

Cyberattacks and other incidents at Virginia colleges and universities remain a significant risk to the commonwealth due to the valuable intellectual property and confidential information at stake. Higher education institutions have a substantial amount of sensitive data related to their functions and the resources necessary to operate their organizations' public safety, law enforcement functions, health facilities, health information systems, payment card processing, intellectual property, student personal information and financial systems. In order to properly protect the data in these institutions, robust information security programs are needed.

As summarized in the chart below, higher education now leads other public entities in all categories of investigations. As these investigations are comprised solely of the MS-ISAC reported issues, the potential exists for additional security incidents to have occurred resulting in a much greater loss. Due to higher education now leading all four investigation categories, we continue to recommend additional guidance for these institutions. It is important to ensure that appropriate governance is established and effective information security programs are implemented in higher education.

Security investigations by category

	Higher education	Local government	Public school systems	COV agencies
Accounts compromised	84%	6%	6%	4%
Malware infections	90%	1%	0%	%
Cyberattacks	50%	22%	0%	28%
Software vulnerabilities	38%	27%	16%	18%
***Potential loss associated with records exposed**	$272,600	$35,278	$60,600	$25,773

*Potential loss associated with records exposed assumes records were exposed and was calculated using the per capita cost of a data breach from the Ponemon Institute's 2017 Cost of a Data Breach Study: Global Analysis report and the number of security investigations.

The commonwealth security incident response team (CSIRT) and CSRM are adjusting the cyber incident response playbooks and other security analysis tools to reflect the new multi-supplier service platform environment.
The playbooks are detailed, written guidance on how the commonwealth will identify, contain, repair and recover from an incident. The playbooks will address the unique requirements of the new multi-supplier service platform environment. This will promote response preparedness, consistency and overall effectiveness of incident response when working with multiple suppliers. These playbooks will be used in our evaluation of agency programs incident response.

State agencies that had previously managed their own infrastructure are moving towards participating in the shared IT infrastructure contracts managed by VITA.
The Virginia Department of Emergency Management (VDEM) and Virginia Employment Commission (VEC) are making plans to transition to the IT infrastructure offerings replacing the Comprehensive Infrastructure Services Agreement (CIA) that will expire in 2018. The new offerings will provide these agencies with all of the benefits of the previous model, including added security and improved incident response processes. In addition, Virginia State Police (VSP) is working with VITA to establish future service offerings to further secure their environment. CSRM recommends that all agencies participate in the enterprise service offerings to ensure adequate enterprise security controls are established to protect agency sensitive records.

CSRM Security Services Center

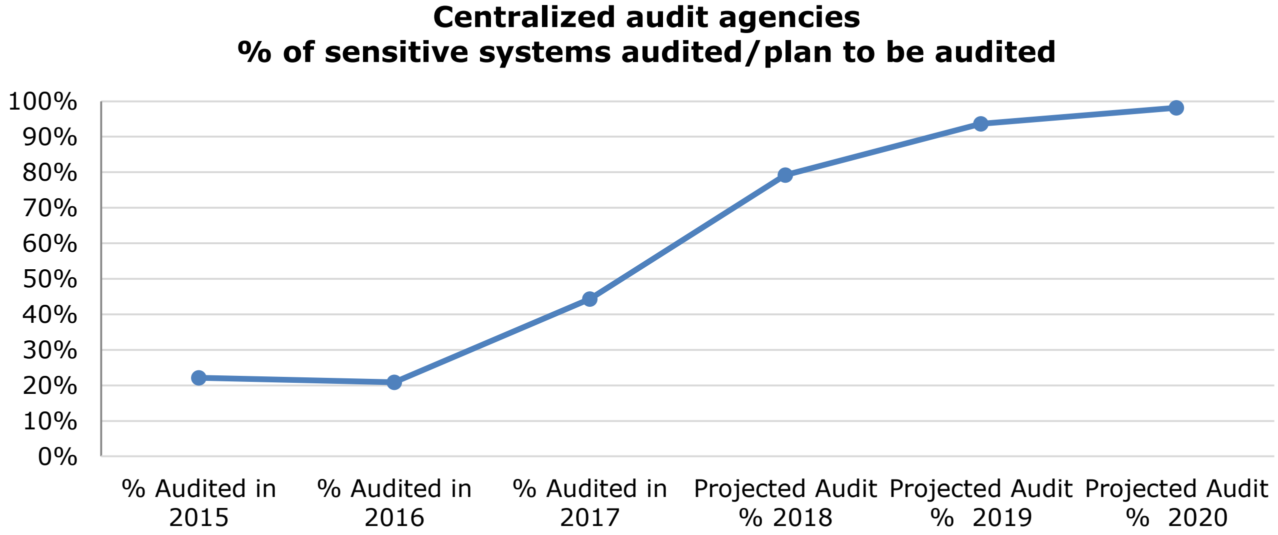
The Security Services Center, also called centralized services, continued to grow in 2017. These services include the IT security audit services, Information Security Officer (ISO) services, and web application vulnerability scanning programs. These services supplement agency IT security programs for the agencies and support of the overall effectiveness of the information security programs in the Commonwealth of Virginia.

Audits
IT security audit
Impact and risk analysis
ISO services
Identifying vulnerabilites
Vulnerablity scanning

IT security audit services

This program finished the calendar year 2017 with 29 signed clients, while building a team of trained, experienced staff. Six agencies were added from the initial 23 that signed up in 2016. This is a 26 percent increase in the number of agencies using centralized audit services. Audits have been completed at 11 agencies and 123 sensitive systems were audited in 2017. After an audit has been completed, IT security audit services continues to work with the agencies to advise them on Corrective Action Plans and scheduling of future audits.

Agencies using IT audit services show marked improvement in the percentage of sensitive systems that have been audited. Based on the audits that are currently scheduled, agencies that are served by VITA IT security audit services are projected to improve their IT security audit compliance metrics and should have fully compliant audit programs by 2020. This will provide further assurance that agencies are aware of any IT security issues related to their sensitive system and develop corrective action plans to address any concerns that are identified.

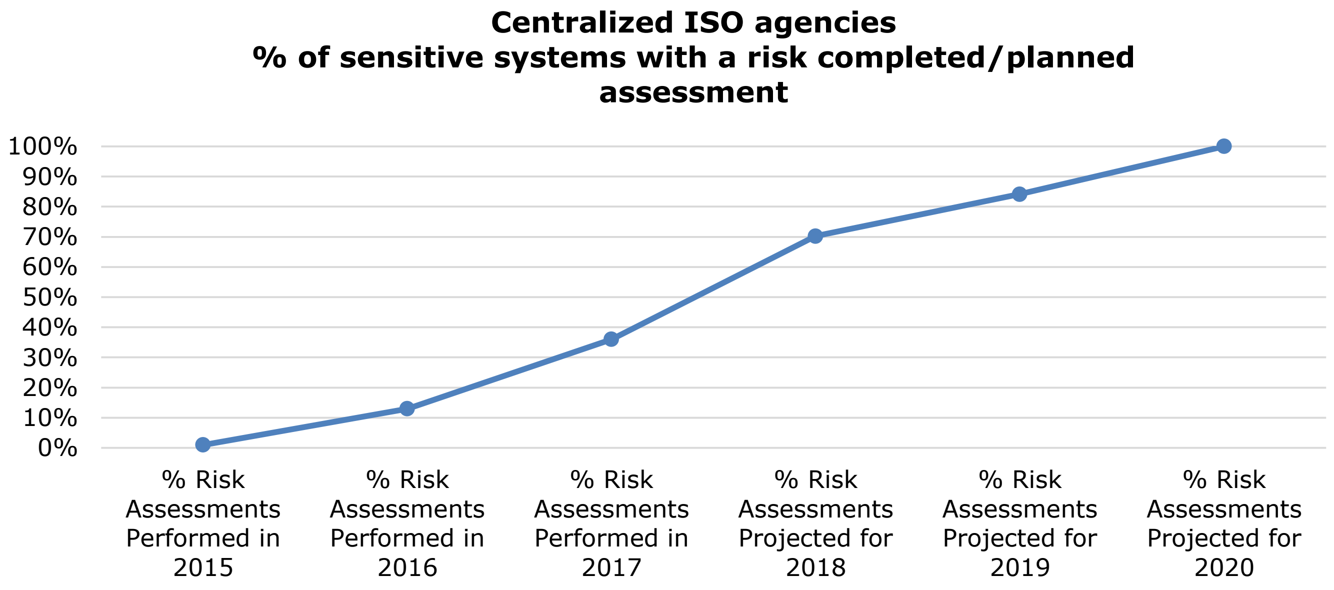


IT audit services also works closely with the ISO service, maintaining professional segregation of information gathered, but sharing knowledge and insight of client applications, environments, and challenges to further promote the security of the commonwealth's information.

ISO services

This program finished calendar year 2017 with 31 signed clients. Six agencies were added from the initial 25 that were signed in 2016. These agencies are all in various stages of their project plan, with some having been working with division staff on multiple levels of support. The past year focus has been to update and report on agency-specific business processes (business impact analysis), documenting IT system risk assessments, responding to IT security audits, and developing agency-specific policies audits have been completed at 11 agencies. After an audit has been completed, we continue to work with the primary contact to advise them on corrective action plans and scheduling of future audits.

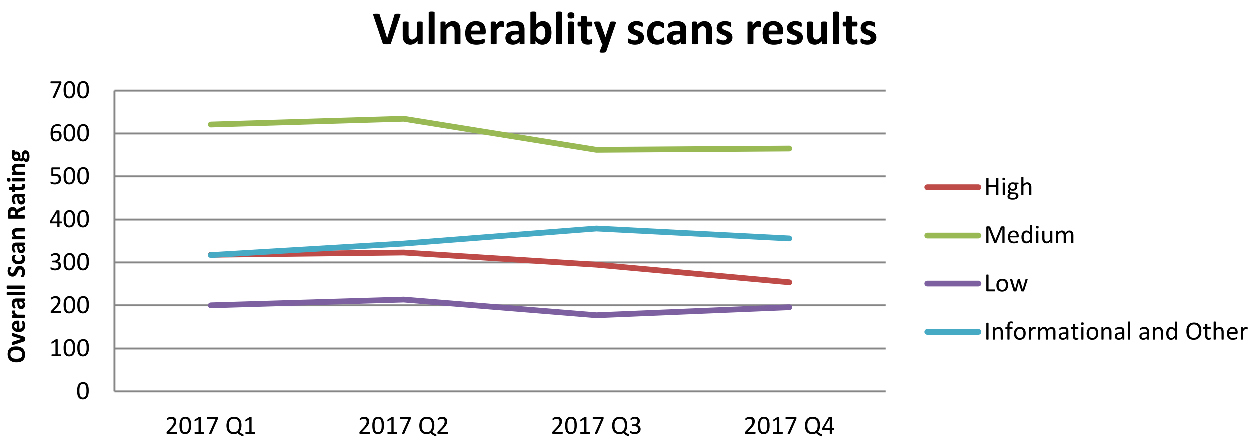
ISO services anticipates a significant improvement in the area of risk assessments. Risk assessments, required by COV standards, help agencies identify, evaluate and prioritize risks and vulnerabilities in commonwealth systems. Agencies then develop risk treatment plans to address these concerns. Based on scheduled risk assessments, ISO services will complete nearly 100 percent of risk assessments for all ISO centralized service agency sensitive systems by 2020.



Web Application Vulnerability Scanning Program

The 2017 Web Application Vulnerability Scanning Program has been underway the full calendar year and is a continually improving service. This service scans public facing websites to identify if there are vulnerabilities that would allow a malicious outsider to attack commonwealth applications and provides these alerts to the agencies so that they can address any weaknesses that are found. Agency cooperation is still high with 99 percent participation. Many components of the web application vulnerability program are constantly changing. The scanning software improves and the alert tests are moved in severity based on the current risks. Scans are conducted once per quarter. The footprint of web applications is further reduced over 2016 by additional decommissions and moving sites behind the perimeter. Agencies have made progress in reducing high vulnerabilities, as well as reducing secure transport related vulnerabilities as well. As the web application vulnerability scanning program matures, CSRM anticipates the program's benefits will be magnified as the result of agencies working to further reduce the commonwealth's attack surface and remediate the changing vulnerabilities to further strengthen commonwealth web application security.

As summarized in the table, the number of vulnerabilities is decreasing over time. In addition, the number of high vulnerabilities is low compared to the medium and informational vulnerabilities. This further confirms that agencies are addressing vulnerabilities, particularly the high vulnerabilities, as they are found.



Commonwealth Information Security Governance Program

The commonwealth's information security governance program is responsible for monitoring performance and compliance against IT security policies and standards, setting security strategy for the commonwealth, supporting agencies in their efforts to foster secure IT security environments, and promoting information security training and awareness.

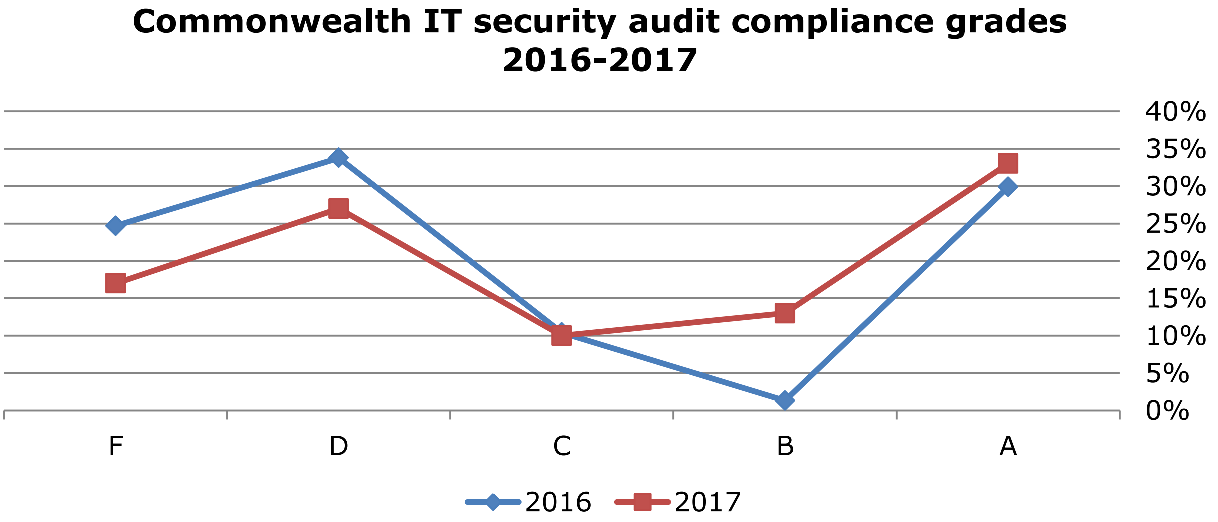
Statute requires compliance monitoring

As directed by §2.2-2009 (B.1) of the Code of Virginia, the CIO is required to report the "results of security audits, the extent to which security policy, standards, and guidelines have been adopted by executive branch and independent agencies, and a list of those executive branch agencies and independent agencies that have not implemented acceptable security and risk management regulations, policies, standards, and guidelines to control unauthorized uses, intrusions, or other security threats." CSRM accomplished this task by monitoring agencies' overall compliance with IT audit program and information security risk program standards and policies. In addition CSRM started transitioning toward a maturity model which provides additional insight into agency programs. This insight will help show where the commonwealth can direct efforts to further the security program.

Audit compliance report card

The compliance report card summarizes agency compliance with the commonwealth's IT security standards, specifically the standards related to IT security audit and risk management. The report card measures each agency's compliance with a letter grade of A, B, C, D, or F to provide a more gradated measurement of agency compliance and more insight into changes in compliance over time.

Overall agency audit programs compliance has improved with the percentage of agencies with grades of A and B increasing from the prior year. CSRM anticipates that compliance will continue to improve that as agencies use the funds afforded them in the biennial budget for IT security, including centralized audit services.



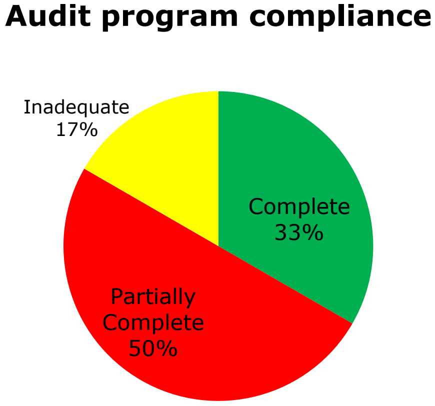
Key commonwealth security audit compliance metrics and analysis

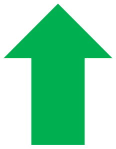
Metrics are summarized below to illustrate the results of IT audit program compliance, security trends, and emerging issues as reported by state agencies.

Commonwealth information security audit program compliance improved in 2017.

IT security audit standards designate that the each agency heads is accountable for their agency cybersecurity programs. Commonwealth standards require agencies to develop and maintain an IT security audit program to evaluate their systems that are deemed sensitive. Agencies are required to develop an IT security audit plan annually, conduct an IT security audit on those systems at a minimum of every three years, and carry out corrective action plans for findings noted during the audits.

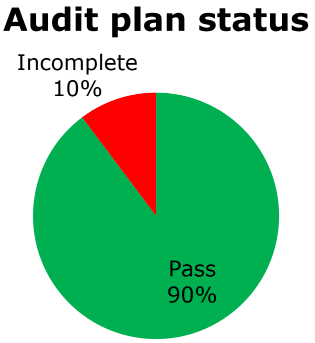
Audit program compliance has improved from the prior year, with 33 percent of agencies having implemented a comprehensive audit program in 2017, compared to 27 percent of agencies with a sufficient audit program last year. Some of the improvement can be attributed to the recent VITA IT security audit services completing audit plans and conducting audits of sensitive systems for agencies that had not had compliant audit programs in the past. In addition, agencies used some IT security funds to complete audits.





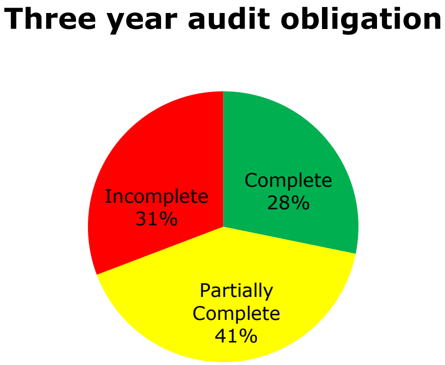
Most agencies are submitting IT security audit plans in accordance with requirements.

Standards require agencies to develop an IT security audit plan that includes all of their sensitive systems with a plan to audit them a minimum of once every three years. Agencies are also required to submit their IT security audit plans to VITA on an annual basis. The IT security audit plans are important because they demonstrate the agencies intentions to complete the audits of their sensitive information systems within the required timeframes. In 2017, two percent more agencies submitted completed IT security audit plans than in the prior year. This increase can be attributed to increased communications with agency to submit the plans when required and was bolstered by agencies joining the IT security audit services and ISO services that assist agencies in developing and submitting these plans.



IT security audit plans submitted increased by 2 percent

While agencies did not consistently complete audits within the required timeframes, overall audit metrics are improving.
Of the agencies that have established an audit plan, 28 percent have fulfilled their obligation to have every sensitive system audited at least once every three years, and 41 percent have partially fulfilled their audit obligation and audited some of their applications. In addition, the percentage of agencies with incomplete program has declined from 40 percent last year to 31 percent this year as agencies begin to meet their audit obligations. As agencies begin to complete their IT security audits with the additional IT security service funding that they have been given and centralized audit servicer, CSRM anticipates this improvement will continue to grow.



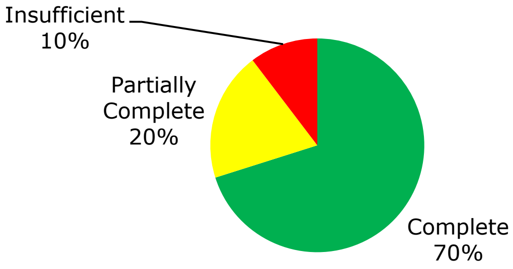
Three year audit obligation completions increased by 1 percent

Agencies did not submit quarterly updates for corrective action plans as they have in prior years.

Standards require agencies to provide quarterly updates to the CISO for corrective action plans with open findings. These updates contain the status of outstanding corrective actions and their expected completion date.

In contrast to the other IT security audit metrics, the percentage of quarterly updates received declined from the prior year. There were nine agencies that did not submit any quarterly updates during the year, contributing to the decline in this metric. As agencies completed more audits, quarterly updates were required. CSRM will further engage and remind/ agencies to submit their quarterly updates to confirm that that issues identified during IT security audits are addressed and ultimately resolved.

Current year percentage of quarterly updates recieved



Quarterly updates received decreased by 17 percent

Commonwealth Information Security Officers Advisory Group

The Information Security Officers Advisory Group (ISOAG) is a dynamic group of information security professionals, open to all state and local government personnel. The group's goal is to exchange IT security knowledge to improve the security posture of the commonwealth. In 2017, CSRM provided knowledgeable speakers from government and private sector organizations to share their information security expertise with the group at no cost to attendees. In addition, the members are able to earn continuing professional education credits (CPE), a requirement necessary for security professionals to maintain their security certifications and memberships in global security organizations, share best practices, provide feedback on proposed policy changes, and are notified of local training opportunities. There was an average of 144 attendees per meeting in 2017, which is a three percent increase in attendance from the prior year. Members can attend the meetings in person or via webinar. Meeting presentation materials are also posted to the VITA website as an additional resource to the group.

Cybersecurity strategy development and monitoring

CSRM has established a cybersecurity strategy to address the security needs for the commonwealth. While the objectives of the strategy have not changed, the tactics to implement the strategy will change to adjust to the multi-supplier environment.

As a part of the cybersecurity strategy, CSRM will continue to be an integral part of the IT strategic planning process to ensure security needs are addressed as part when considering investing in new technologies.

Governance also plays a role in cybersecurity strategy. The commonwealth's IT security governance program is formally documented in one policy and five standards designed to assist agencies in building and documenting their individual security programs. The policy sets the commonwealth’s overall direction and establishes a framework that agency heads must follow in implementing IT security programs. In addition, templates are also available to help agencies develop their own policies.

In 2017, CSRM reviewed and proposed updates for SEC-501 ”IT Information Security Standard” and SEC-525 “Hosted Environment Security Standard”. Changes were related to penetration testing, data center minimum requirements, and refining the existing guidance. A more extensive update will be done in the upcoming year.

Commonwealth Information Security (IS) Council

The Commonwealth IS Council is comprised of members from various state agencies who provide input for the direction of the commonwealth-wide information security program and raise information security awareness within the commonwealth. The IS Council meets bi-monthly. In 2017, the council worked on various initiatives, including the ISO knowledge sharing website. CSRM extends is gratitude to the IS Council for their work and support of the highly successful 2017 COV Information Security Conference. The Council is taking on a new key role that will include risk management responsibilities. The Council will provide input and assist in evaluating the risk management priorities for the commonwealth.

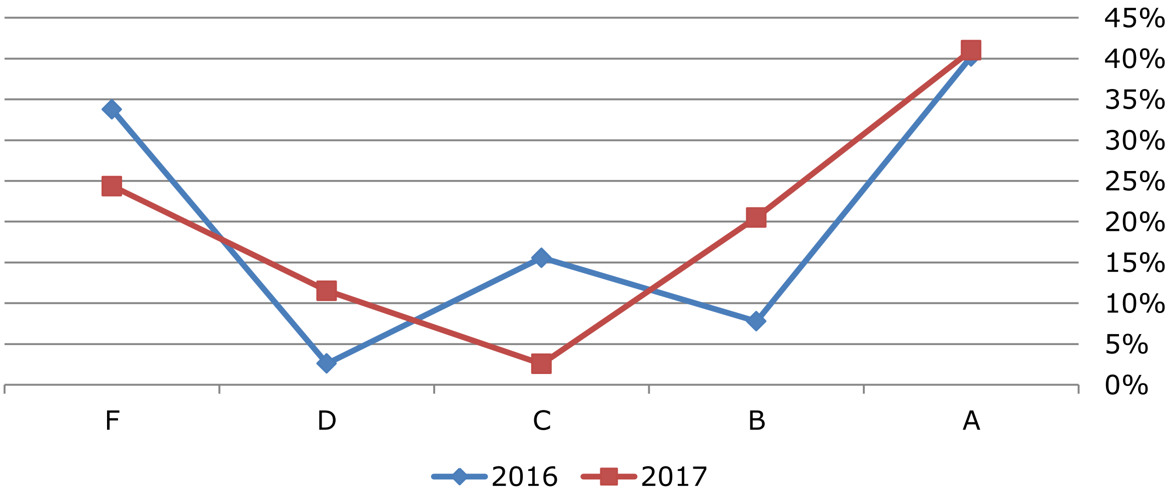
Commonwealth IT risk management program

The commonwealth IT risk management program provides oversight of the agencies’ risk management programs, including submission of their BIA, risk assessments, and intrusion detection reporting. In addition, CSRM collected sets of data from agencies’ existing BIAs, risk assessments and data on vulnerabilities and threats. These data are used to develop the commonwealth’s overall risk program score, which indicates that more than half of the agencies have an insufficient risk management program.

Risk compliance report card

Overall risk compliance has improved as well. The percentage of agencies with grades of A and B also increased from the prior year. CSRM anticipates the risk program compliance will continue to increase with agencies using the centralized ISO service and dedicating IT resources toward their risk management programs.

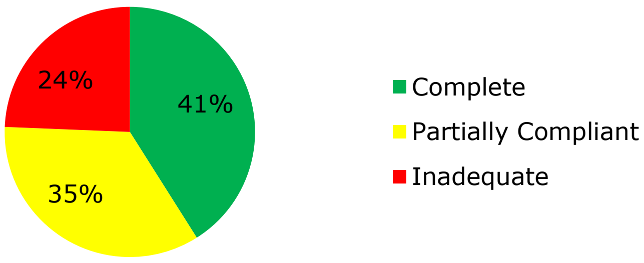
Commonwealth risk compliance grades 2016-2017

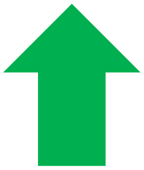


IT risk management program monitoring

Risk management program compliance has improved.
Risk management program compliance has increased five percent, up from 36 percent of agencies having implemented a comprehensive risk management program. The increase can be attributed in part to additional funding made available to the agencies for their IT security program and centralized ISO services who completed risk assessment plans, risk assessments, and business impact analysis (BIA) in support of the agency's risk programs. Agencies should continue to conduct their risk assessments and complete their BIA's to grow the overall agency compliance. CSRM recommends that agencies support risk management efforts by dedicating the necessary resources to their IT risk management programs.

Risk program compliance



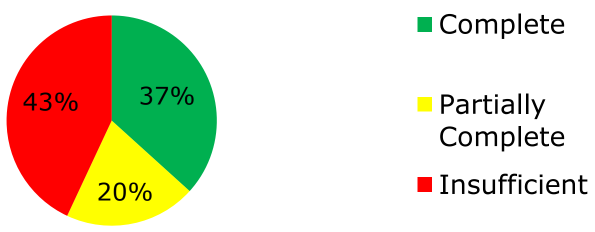


Overall risk program compliance increased by 5 percent

Three year risk assessment obligation compliance has improved; however, most agencies still have not met this obligation.
Agencies are required by SEC520-00.1 to review their risk assessment plans for the IT systems for which they are the data owner on an annual basis. The risk assessment is the process of identifying vulnerabilities, threats, likelihood of occurrence and potential loss or impact. There were 26 agencies (34 percent) that provided complete risk assessment information. Of the 77

agencies, 51 agencies (66 percent) did not fully complete the required risk assessment information.

Three year risk assessment obligation



Three year risk assessment obligation decreased by 3 percent

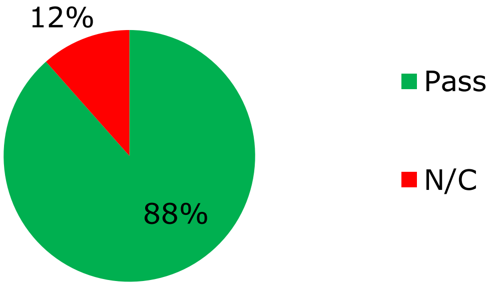
The percentage of certified ISO personnel working at the agencies has remained the same.

Certification is one way to provide assurance that agency IT personnel are trained and equipped to manage agency IT security programs. The commonwealth ISO certification demonstrates that personnel have received annual information security training and have some knowledge of commonwealth information security practices. Agencies that do not have a certified ISO have an average IT security audit compliance grade of F and an average risk management grade of F. The following agencies do not have certified ISOs at the conclusion of 2017:

- Tobacco Region Revitalization Commission
- Virginia Resources Authority
- Southwest Virginia Higher Education Center
- Virginia Commission for the Arts
- Virginia School for the for Deaf and Blind
- Virginia Museum of Fine Arts
- Office of the Attorney General
- Virginia Foundation for Healthy Youth
- Commonwealth’s Attorney’s Service Council

CSRM strongly recommends that these agencies recruit and hire capable and certified ISO staff to improve their agencies IT security posture.

% of ISO's that are certified in the commonwealth

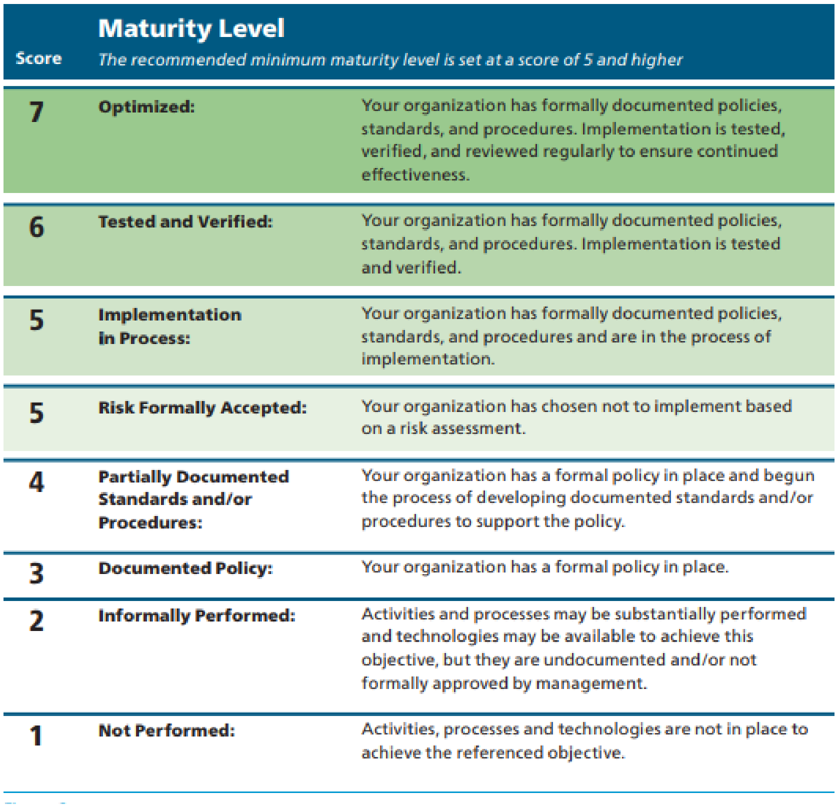


No change in the percentage of certified ISOs

Nationwide Cyber Security Review

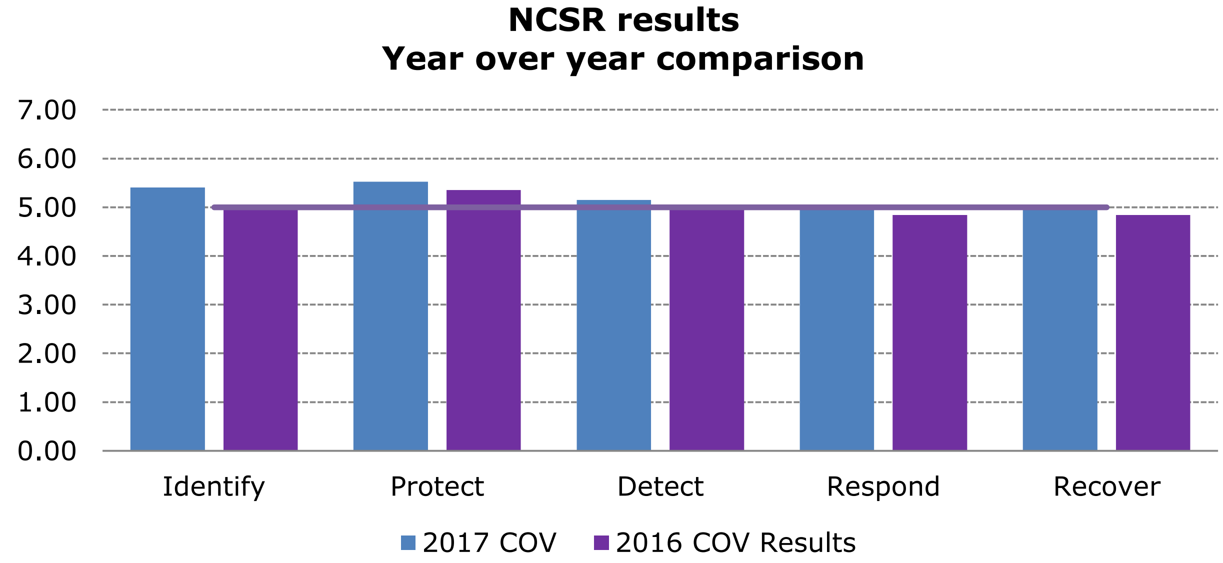
CSRM encouraged agency participation in the Nationwide Cyber Security Review (NCSR), a cyber network security assessment designed to measure security gaps and capabilities.
The NCSR questions are built on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) core, with some minor alterations. The assessment provides a point in time analysis based on the agency's self-assessment of their processes and controls. The core consists of a collection of cybersecurity related activities organized into five main functions: Identify, Protect, Detect, Respond and Recover. Each function is subdivided into categories and then further into subcategories.

There were 39 agencies in the commonwealth that participated in this this extensive assessment, a decline in the number of agencies who participated last year, who evaluated the maturity level of their processes and controls using the scoring described in the table below from the Nationwide Cyber Security Review.

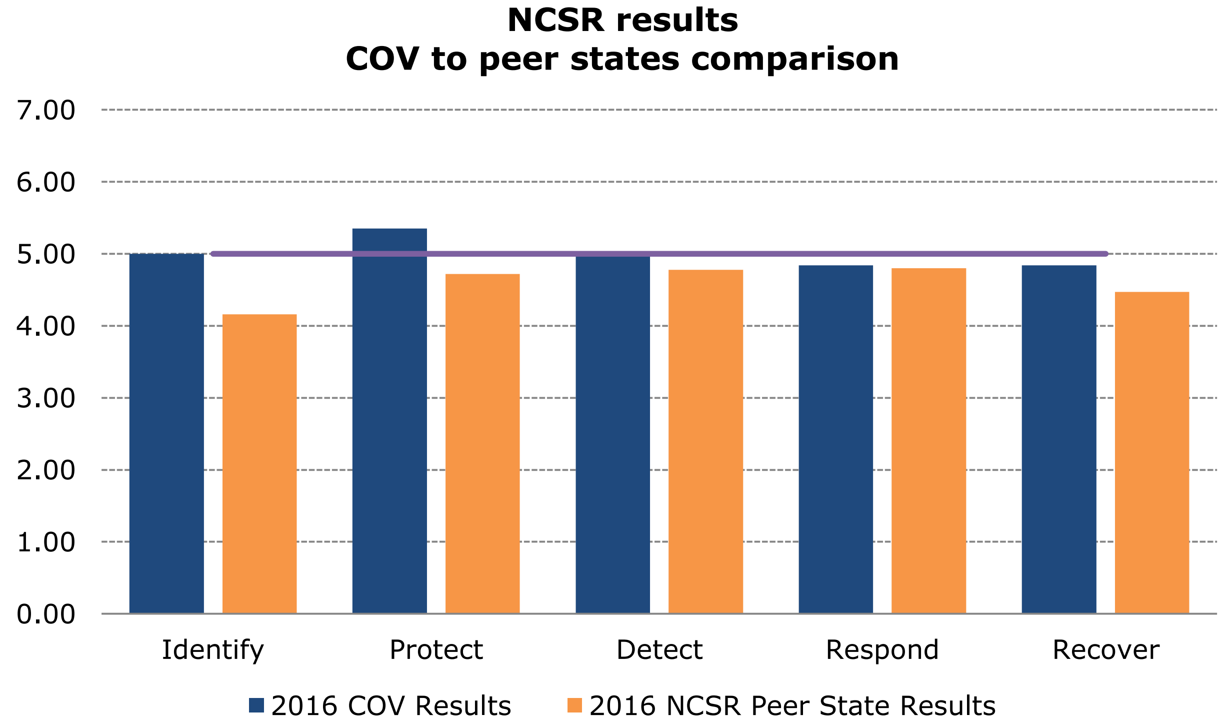


Score	**Maturity Level** *The recommended minimum maturity level is set at a score of 5 and higher*	
7	**Optimized:**	Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified:**	Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process:**	Your organization has formally documented policies, standards, and procedures and are in the process of implementation.
5	**Risk Formally Accepted:**	Your organization has chosen not to implement based on a risk assessment.
4	**Partially Documented Standards and/or Procedures:**	Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy:**	Your organization has a formal policy in place.
2	**Informally Performed:**	Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed:**	Activities, processes and technologies are not in place to achieve the referenced objective.

Overall commonwealth results were optimistic.
For the agencies that participated, the protect function is the most mature function and recover is the least mature function in 2017. This is consistent with the results from the prior year. As noted in the table above, the recommended minimum maturity level is a score of five or higher and the commonwealth meets this minimum criterion for every function in the CSF. This indicates that agencies reported that the implementation of policies, standards, and procedures are generally in process for all of the functions in the framework.



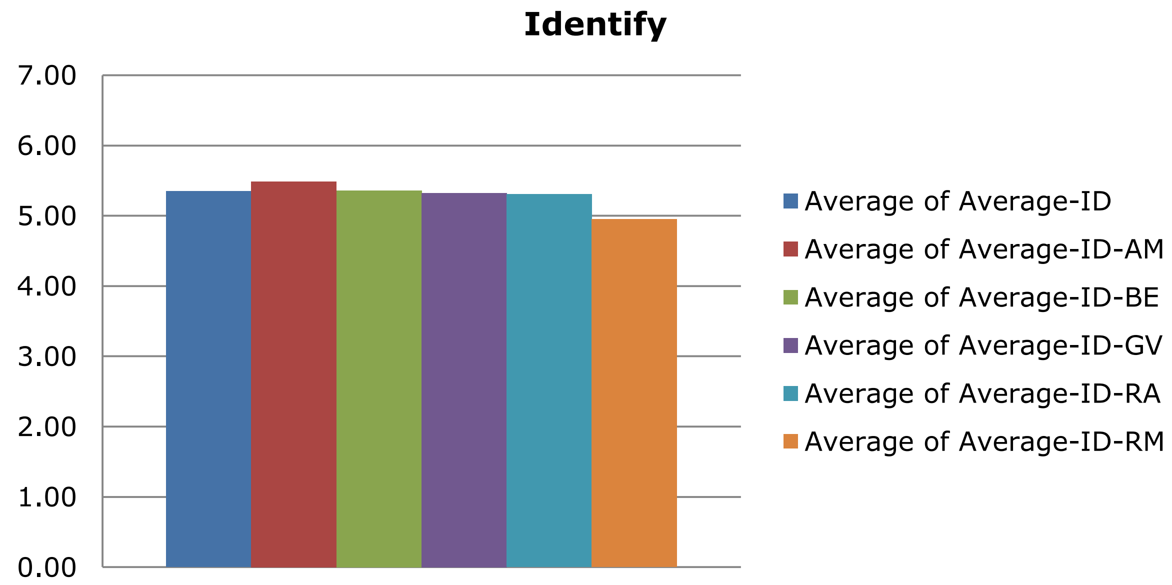
Commonwealth agencies compared favorably with their peers in other states. The results demonstrate that the commonwealth agencies reported maturity levels significantly higher than the maturity level of peer state agencies that took part in the survey in 2016 for every function in the framework. The most significant difference is found in the identify function, where commonwealth agencies reported they were 20 percent more mature than their peer agencies on average.



Cybersecurity framework – analysis by function

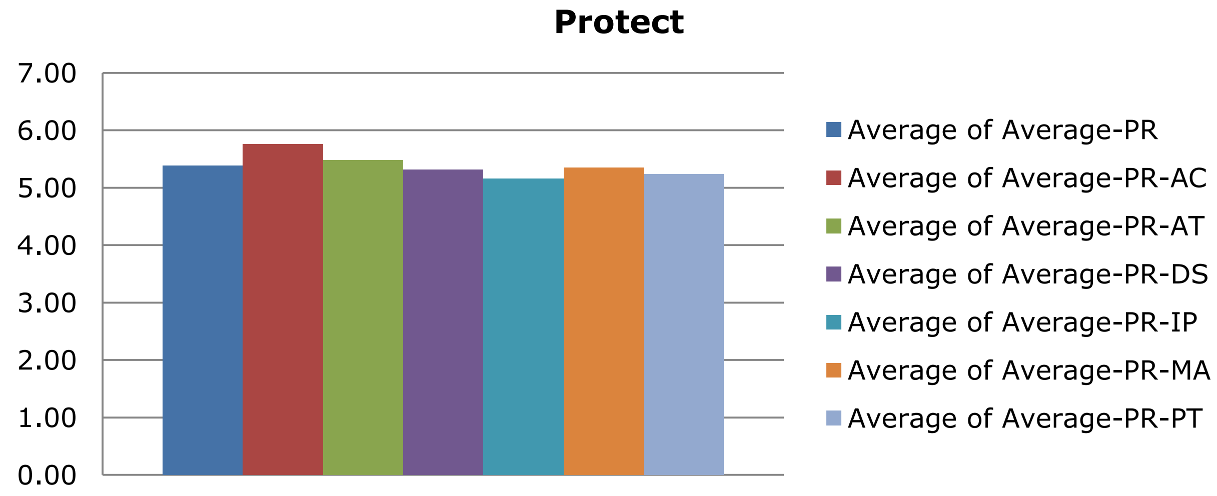
Identify

This function includes asset management (AM), business environment (BE), governance (GV), risk assessment (RA) and risk management (RM) strategy. In 2017, agencies reported that the commonwealth is most mature in the Asset Management category and least mature in the RM strategy category. CSRM will continue to focus on the risk assessment requirements and encourage agencies to better the risks as they are identified.



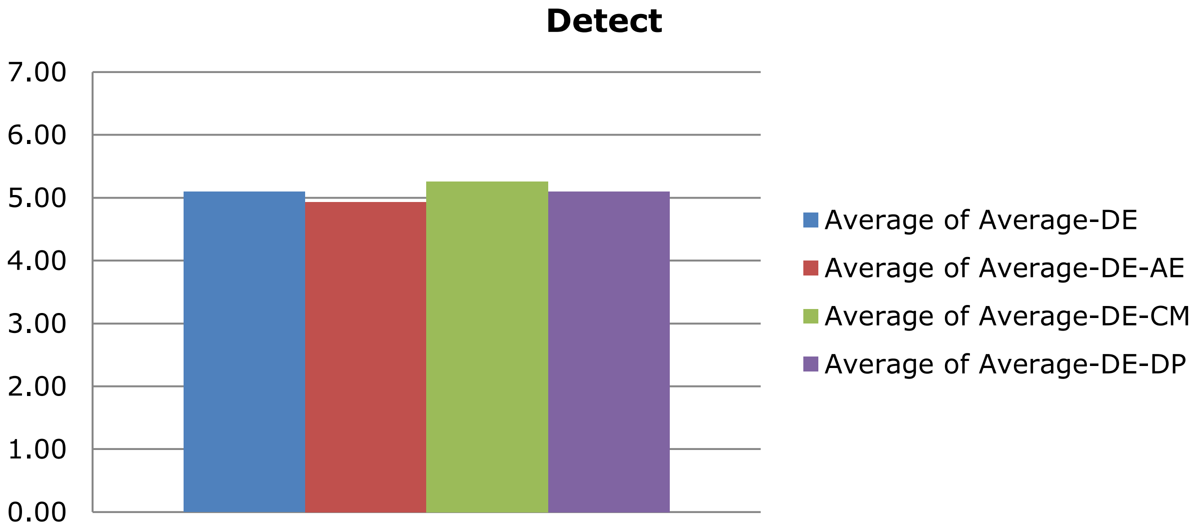
Protect

This function includes access control (AC), awareness and training (AT), data security (DS), information protection processes and procedures (IP), maintenance (MA), and protective technology (PT). Agencies report they were strongest in the AC category and the weakest in the IP category. CSRM will continue to support agencies as they develop in that area.



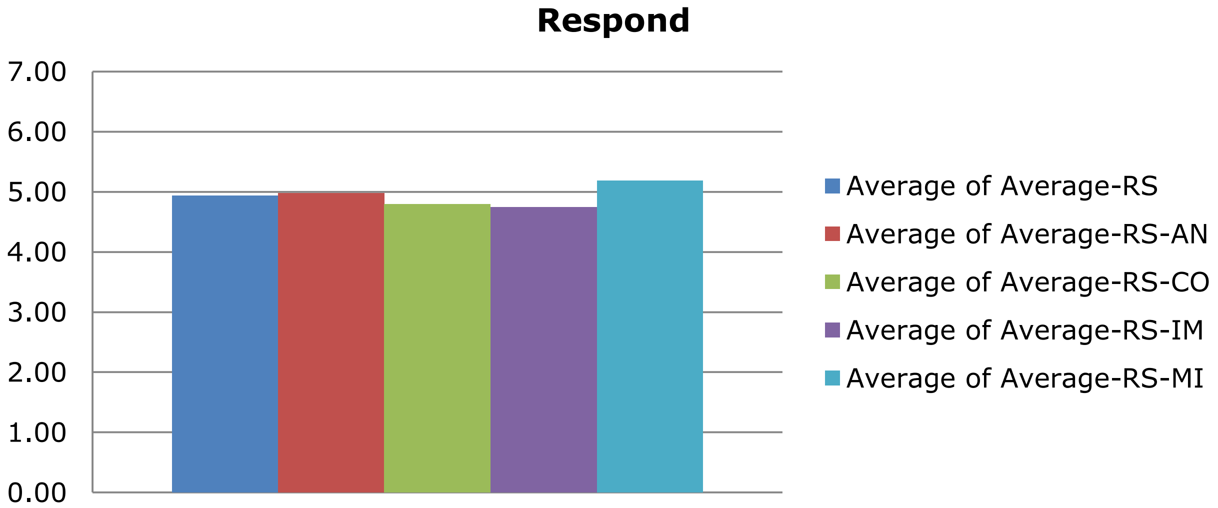
Detect

This function includes categories for anomalies and events (AE), security continuous monitoring (CM), and detection processes (DP). Agencies reported that the CM category was the most mature and the AE was the least mature part of this function, indicating that agencies were less confident that anomalies would be identified timely. New enterprise partners and updated security tools should result in further improvement in this area.



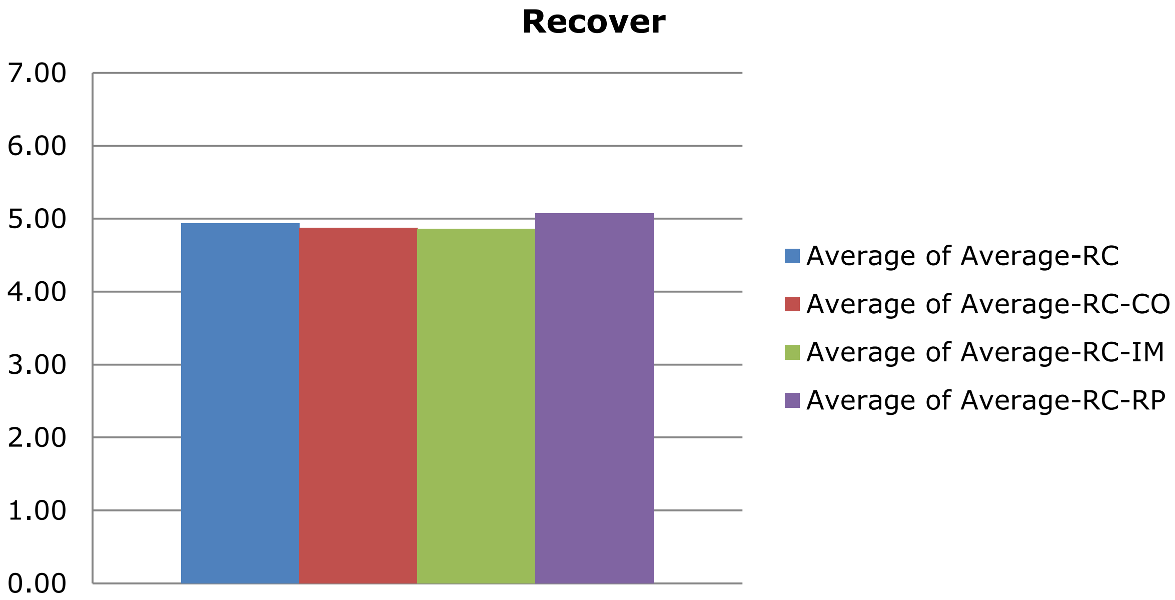
Respond

The categories for respond (RS) are response planning (RP), communications (CO), analysis (AN), mitigations (MI), and improvements (IM). The agencies reported that they are strongest on average in the MI category and indicated that the CO category was the least mature category in the function. New enterprise security tools will assist in improving some of the communication for responses.



Recover

This function includes recovery planning (RP), improvements (IM), and communications (CO). The results were very similar for all of the categories, with the RP category being slightly more mature and IM being slightly less mature than the other categories. The overall recover function needs improvement to reach the desired level for the commonwealth.


Recover
7.00
6.00
5.00
4.00
3.00
2.00
1.00
0.00
🟦 Average of Average-RC
🟥 Average of Average-RC-CO
🟩 Average of Average-RC-IM
🟪 Average of Average-RC-RP

Appendix I –Agency compliance report card

* Agency is a part of one centralized service (audit or ISO)
** Agency participates in both the centralized audit service and the centralized ISO service

	Agency Secretariat	Audit or ISO Services?	Agency Acronym	Audit Compliance Grade	Risk Compliance Grade
**	Administration	Audit, ISO	CB	A	B
	Administration		DGS	D	A
**	Administration	Audit, ISO	DHRM	C	A
*	Administration	ISO	ELECT	A	A
**	Agriculture & Forestry	Audit, ISO	DOF	C	B
	Agriculture & Forestry		VDACS	A	A
**	Commerce and Trade	Audit, ISO	BOA	B	A
*	Commerce and Trade	Audit	DHCD	D	D
**	Commerce and Trade	Audit, ISO	DMME	D	B
**	Commerce and Trade	Audit, ISO	DOLI	B	A
	Commerce and Trade		DPOR	B	D
**	Commerce and Trade	Audit, ISO	SBSD	A	A
	Commerce and Trade		TIC	D	F
	Commerce and Trade		VEC	B	D
	Commerce and Trade		VEDP	D	F
	Commerce and Trade		VRA	F	F
**	Commerce and Trade	Audit, ISO	VRC	C	B
*	Education	Audit	DOE	B	D
*	Education	ISO	FCMV	D	B
*	Education	ISO	GH	A	A
**	Education	Audit, ISO	JYF	D	B
	Education		LVA	D	A
**	Education	Audit, ISO	NSU	C	F
	Education		RBC	F	F
**	Education	Audit, ISO	SCHEV	C	C
*	Education	ISO	SMV	A	B
*	Education	ISO	SVHEC	A	B
	Education		SWVHEC	F	F
	Education		VCA	F	F
*	Education	Audit	VMFA	F	F
	Education		VSDB	F	F
**	Education	Audit, ISO	VSU	A	A
*	Executive	ISO	GOV	D	A
	Executive		OAG	F	F
	Executive		OSIG	A	A
*	Finance	Audit	DOA	A	A
**	Finance	Audit, ISO	DPB	D	A

Appendix I - Agency Information Security Data Points –Agency Compliance Report Card

	Agency Secretariat	Audit or ISO Services?	Agency Acronym	Audit Compliance Grade	Risk Compliance Grade
	Finance		TAX	B	B
	Finance		TD	A	A
	Health and Human Resources		CSA	D	A
	Health and Human Resources		DARS	A	B
	Health and Human Resources		DBHDS	F	A
*	Health and Human Resources	Audit	DDHH	D	A
	Health and Human Resources		DHP	A	B
	Health and Human Resources		DMAS	B	D
	Health and Human Resources		DSS	F	F
	Health and Human Resources		VDH	B	A
	Health and Human Resources		VFHY	F	F
**	Independent	Audit, ISO	IDC	D	F
	Independent		SCC	A	C
	Independent		SLD	D	F
	Independent		VCSP	A	A
	Independent		VRS	A	F
*	Independent	Audit	VWC	A	A
*	Natural Resources	ISO	DCR	A	A
**	Natural Resources	Audit, ISO	DEQ	A	B
*	Natural Resources	ISO	DGIF	C	B
**	Natural Resources	Audit, ISO	DHR	D	A
*	Natural Resources	Audit	MRC	A	A
**	Natural Resources	Audit, ISO	VMNH	A	A
	Public Safety		ABC	B	F
	Public Safety		CASC	A	D
**	Public Safety	Audit, ISO	DCJS	D	B
	Public Safety		DFP	C	B
**	Public Safety	Audit, ISO	DFS	D	A
*	Public Safety	ISO	DJJ	A	A
	Public Safety		DMA	F	F
	Public Safety		DOC	A	A
	Public Safety		DVS	A	A
	Public Safety		VDEM	D	F
**	Public Safety	Audit, ISO	VSP	D	D
	Technology		IEIA	A	A
**	Technology	Audit, ISO	VITA	C	B
	Transportation		DMV	D	A
	Transportation		DOAV	A	A
*	Transportation	Audit	DRPT	F	F

Appendix I - Agency Information Security Data Points –Agency Compliance Report Card

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Audit Compliance Grade	Risk Compliance Grade
** Transportation	Audit, ISO	MVDB	D	B
Transportation		VDOT	B	D

Appendix II - Agency information security data points
Agency information security data points detail - Legend

Audit and/or ISO shared services

Audit -Participated in VITA IT security audit service
ISO -Participated in VITA ISO program
Audit, ISO -Agency used both IT Security and audit services

Audit plan status

Pass - Documents received as scheduled
N/C - Missing audit plan

Current year percentage of audit reports received

X% - The percentage of due audit reports received based on the security audit plan
N/A - Not applicable as the agency had no audits due
N/C - The agency head has not submitted a complete IT security audit plan

Current year percentage of quarterly updates received

X% - The percentage of due corrective action plans and quarterly updates received based on the security audit plan
N/A - Not applicable as the agency had no quarterly updates due or the agency head has not submitted a security audit plan

Three year audit obligation

X% - The percentage of audit work completed as measured against the agency's security audit plans over the past three years
N/A - Not applicable as the agency had no audits due
N/C - The agency head has not submitted a security audit plan

Risk assessment plan status

Pass - Documents received as scheduled
N/C - Missing risk assessment plan

Three year risk assessment obligation completed

X% - The percentage of risk assessment work completed as measured against the agency's sensitive systems over the past three years
N/A - Not applicable as the agency had no risk assessments due
N/C - The agency head has not submitted an audit plan

2017 business impact analysis status

Pass - All documentation received as requested
Incomplete - Documentation received, but incomplete
N/C - Documentation was not submitted

IDS quarterly reports

Pass - Documents received as scheduled
N/C - Reports were not received

Data set inventory

Compliant - Data set information was provided
Non-Compliant- Data set information was not provided fully

ISO certification status

Pass - The primary ISO is certified
Incomplete - The ISO met all other requirements but did not attend the mandatory ISOAG meeting
N/C - The primary ISO is NOT certified

Agency secretariat	Agency acronym	Audit and/or ISO shared services	Audit plan status	Current year percentage of audit reports received	Current year percentage of quarterly updates received	Three year audit obligation	Risk assessment plan status	Three year risk assessment obligation	BIA status	IDS quarterly reports	Data set inventory	ISO certification status
Administration	CB	Audit, ISO	Pass	0%	N/A	0%	Pass	N/C	100%	Pass	Compliant	Pass
Administration	DGS		Pass	100%	N/A	8%	Pass	50%	100%	Pass	Compliant	Pass
Administration	DHRM	Audit, ISO	Pass	N/A	100%	30%	Pass	100%	100%	Pass	Compliant	Pass
Administration	ELECT	ISO	Pass	N/A	100%	100%	Pass	100%	100%	Pass	Compliant	Pass
Agriculture & Forestry	DOF	Audit, ISO	Pass	0%	100%	53%	Pass	0%	100%	Pass	Compliant	Pass
Agriculture & Forestry	VDACS		Pass	100%	100%	95%	Pass	100%	100%	Pass	Compliant	Pass
Commerce and Trade	BOA	Audit, ISO	Pass	N/A	100%	50%	Pass	100%	100%	Pass	Compliant	Pass
Commerce and Trade	DHCD	Audit	Pass	100%	0%	100%	N/C	N/C	100%	Pass	Compliant	Pass
Commerce and Trade	DMME	Audit, ISO	Pass	N/A	100%	0%	Pass	0%	100%	Pass	Compliant	Pass
Commerce and Trade	DOLI	Audit, ISO	Pass	100%	100%	44%	Pass	100%	100%	Pass	Compliant	Pass
Commerce and Trade	DPOR		Pass	N/A	50%	100%	Pass	0%	0%	Pass	Compliant	Pass
Commerce and Trade	SBSD	Audit, ISO	Pass	75%	N/A	75%	Pass	100%	100%	Pass	Compliant	Pass
Commerce and Trade	TIC		Pass	0%	0%	N/A	N/C	N/C	0%	Pass	Compliant	N/C
Commerce and Trade	VEC		Pass	100%	100%	52%	Pass	0%	100%	Pass	Non-Compliant	Pass

Agency secretariat	Agency acronym	Audit and/or ISO shared services	Audit plan status	Current year percentage of audit reports received	Current year percentage of quarterly updates received	Three year audit obligation	Risk assessment plan status	Three year risk assessment obligation	BIA status	IDS quarterly reports	Data set inventory	ISO certification status
Commerce and Trade	VEDP		Pass	0%	N/A	0%	N/C	N/C	N/C	Fail	Compliant	Pass
Commerce and Trade	VRA		N/C	N/C	0%	N/C	N/C	N/C	N/C	Pass	Partial	N/C
Commerce and Trade	VRC	Audit, ISO	Pass	100%	N/A	33%	Pass	0%	100%	Pass	Compliant	Pass
Education	DOE	Audit	Pass	0%	75%	89%	Pass	0%	N/C	Pass	Compliant	Pass
Education	FCMV	ISO	Pass	N/A	N/A	0%	Pass	100%	100%	Pass	Non-Compliant	Pass
Education	GH	ISO	Pass	N/A	N/A	N/A	Pass	N/A	100%	Pass	Compliant	Pass
Education	JYF	Audit, ISO	Pass	0%	N/A	0%	Pass	17%	100%	Pass	Compliant	Pass
Education	LVA		Pass	0%	100%	0%	Pass	100%	100%	Pass	Compliant	Pass
Education	NSU	Audit, ISO	Pass	N/A	N/A	24%	Pass	N/C	N/C	Pass	Non-Compliant	Pass
Education	RBC		Pass	0%	0%	67%	N/C	N/C	N/C	Pass	Compliant	Pass
Education	SCHEV	Audit, ISO	Pass	100%	25%	100%	Pass	0%	25%	Pass	Compliant	Pass
Education	SMV	ISO	Pass	N/A	N/A	100%	Pass	N/C	100%	Pass	Compliant	Pass
Education	SVHEC	ISO	Pass	N/A	N/A	N/A	Pass	N/A	100%	Fail	Compliant	Pass
Education	SWVHEC		N/C	N/C	N/A	N/C	N/C	N/C	N/C	Fail	Non-Compliant	N/C
Education	VCA		N/C	N/C	N/A	N/C	N/C	N/C	0%	Pass	Partial	N/C
Education	VMFA	Audit	Pass	0%	0%	0%	N/C	N/C	100%	Pass	Compliant	N/C
Education	VSDB		N/C	N/C	0%	N/C	N/C	N/C	N/C	Pass	Compliant	N/C
Education	VSU	Audit, ISO	Pass	100%	100%	72%	Pass	79%	100%	Pass	Compliant	Pass

Agency secretariat	Agency acronym	Audit and/or ISO shared services	Audit plan status	Current year percentage of audit reports received	Current year percentage of quarterly updates received	Three year audit obligation	Risk assessment plan status	Three year risk assessment obligation	BIA status	IDS quarterly reports	Data set inventory	ISO certification status
Executive	GOV	ISO	Pass	N/A	N/A	0%	Pass	100%	100%	Pass	Compliant	Pass
Executive	OAG		N/C	N/C	50%	N/C	N/C	N/C	N/C	Pass	Non-Compliant	N/C
Executive	OSIG		Pass	N/A	100%	100%	Pass	100%	100%	Pass	Compliant	Pass
Finance	DOA	Audit	Pass	100%	100%	89%	Pass	94%	100%	Pass	Compliant	Pass
Finance	DPB	Audit, ISO	Pass	N/A	N/A	0%	Pass	100%	100%	Pass	Compliant	Pass
Finance	TAX		Pass	63%	100%	68%	Pass	33%	100%	Pass	Partial	Pass
Finance	TD		Pass	100%	100%	90%	Pass	100%	100%	Pass	Compliant	Pass
Health and Human Resources	CSA		Pass	N/A	0%	100%	Pass	100%	100%	Pass	Compliant	Pass
Health and Human Resources	DARS		Pass	100%	100%	93%	Pass	20%	100%	Pass	Compliant	Pass
Health and Human Resources	DBHDS		Pass	41%	43%	6%	Pass	82%	100%	Pass	Compliant	Pass
Health and Human Resources	DDHH	Audit	Pass	N/A	N/A	0%	Pass	100%	100%	Pass	Compliant	Pass
Health and Human Resources	DHP		Pass	100%	100%	100%	Pass	100%	12%	Pass	Compliant	Pass
Health and Human Resources	DMAS		Pass	90%	100%	44%	Pass	0%	0%	Pass	Compliant	Pass
Health and Human Resources	DSS		N/C	N/C	0%	49%	N/C	4%	N/C	Pass	Compliant	Pass
Health and Human Resources	VDH		Pass	88%	100%	49%	Pass	89%	100%	Pass	Compliant	Pass

Agency secretariat	Agency acronym	Audit and/or ISO shared services	Audit plan status	Current year percentage of audit reports received	Current year percentage of quarterly updates received	Three year audit obligation	Risk assessment plan status	Three year risk assessment obligation	BIA status	IDS quarterly reports	Data set inventory	ISO certification status
Health and Human Resources	VFHY		N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Non-Compliant	N/C
Independent	IDC	Audit, ISO	Pass	N/A	N/A	N/C	N/C	N/C	0%	Pass	Compliant	Pass
Independent	SCC		Pass	83%	100%	82%	Pass	0%	100%	Pass	Partial	Pass
Independent	SLD		Pass	0%	100%	21%	Pass	N/C	N/C	Fail	Non-Compliant	Pass
Independent	VCSP		Pass	100%	100%	100%	Pass	100%	100%	Pass	Compliant	Pass
Independent	VRS		Pass	100%	100%	100%	N/C	N/C	N/C	Pass	Compliant	Pass
Independent	VWC	Audit	Pass	100%	N/A	100%	Pass	100%	100%	Pass	Compliant	Pass
Natural Resources	DCR	ISO	Pass	N/A	N/A	75%	Pass	50%	100%	Pass	Compliant	Pass
Natural Resources	DEQ	Audit, ISO	Pass	100%	100%	100%	Pass	0%	100%	Pass	Compliant	Pass
Natural Resources	DGIF	ISO	Pass	N/A	N/A	35%	Pass	19%	100%	Pass	Compliant	Pass
Natural Resources	DHR	Audit, ISO	Pass	N/A	N/A	0%	Pass	100%	100%	Pass	Compliant	Pass
Natural Resources	MRC	Audit	Pass	N/A	N/A	100%	Pass	100%	100%	Pass	Compliant	Pass
Natural Resources	VMNH	Audit, ISO	Pass	100%	N/A	100%	Pass	100%	100%	Pass	Compliant	Pass
Public Safety	ABC		Pass	100%	100%	59%	Pass	0%	N/C	Pass	Partial	Pass
Public Safety	CASC		Pass	N/A	N/A	N/A	Pass	N/A	100%	Pass	Non-Compliant	N/C
Public Safety	DCJS	Audit, ISO	Pass	N/A	N/A	0%	Pass	0%	100%	Pass	Compliant	Pass
Public Safety	DFP		Pass	50%	100%	38%	Pass	25%	100%	Pass	Compliant	Pass

Agency secretariat	Agency acronym	Audit and/or ISO shared services	Audit plan status	Current year percentage of audit reports received	Current year percentage of quarterly updates received	Three year audit obligation	Risk assessment plan status	Three year risk assessment obligation	BIA status	IDS quarterly reports	Data set inventory	ISO certification status
Public Safety	DFS	Audit, ISO	Pass	N/A	N/A	0%	Pass	100%	100%	Pass	Compliant	Pass
Public Safety	DJJ	ISO	Pass	N/A	100%	100%	Pass	100%	100%	Pass	Compliant	Pass
Public Safety	DMA		N/C	N/C	N/A	N/C	N/C	N/C	N/C	Pass	Compliant	Pass
Public Safety	DOC		Pass	60%	100%	79%	Pass	100%	100%	Pass	Compliant	Pass
Public Safety	DVS		Pass	100%	N/A	100%	Pass	100%	100%	Pass	Compliant	Pass
Public Safety	VDEM		Pass	N/A	N/A	0%	N/C	N/C	N/C	Pass	Compliant	Pass
Public Safety	VSP	Audit, ISO	Pass	0%	100%	7%	N/C	N/C	100%	Pass	Compliant	Pass
Technology	IEIA		Pass	N/A	100%	100%	Pass	100%	100%	Pass	Partial	Pass
Technology	VITA	Audit, ISO	Pass	100%	100%	32%	Pass	53%	100%	Pass	Partial	Pass
Transportation	DMV		Pass	0%	75%	25%	Pass	85%	100%	Pass	Compliant	Pass
Transportation	DOAV		Pass	N/A	100%	100%	Pass	100%	100%	Pass	Compliant	Pass
Transportation	DRPT	Audit	Pass	N/A	0%	0%	N/C	N/C	N/C	Pass	Compliant	Pass
Transportation	MVDB	Audit, ISO	Pass	N/A	N/A	0%	Pass	0%	100%	Pass	Compliant	Pass
Transportation	VDOT		Pass	100%	69%	84%	Pass	65%	N/C	Pass	Partial	Pass

Appendix III – Cybersecurity framework results – Detail

National Cyber Security Review (NCSR) Results

Maturity Level Legend

7 – Optimized
6 – Tested and Verified
5 – Implementation in Process
5 – Risk Formally Accepted
4 –Partially Documented Standards and/or Procedures
3 – Documented Policy
2- Informally Performed
1 - Not Performed
0 -Agency did not complete the survey
** Recommended maturity level is 5 or higher*

Agency Name	Detect	Identify	Protect	Recover	Respond
Alcoholic Beverage Control	0.00	0.00	0.00	0.00	0.00
Board of Accountancy	5.73	5.72	5.65	5.44	5.36
Center for Innovative Technologies	2.75	4.95	5.42	2.67	2.38
Commonwealths Attorneys Services Council	0.00	0.00	0.00	0.00	0.00
Compensation Board	5.32	5.37	5.73	5.72	5.68
Department for Aging and Rehabilitative Services	6.00	5.33	5.96	5.56	5.74
Department for the Deaf and Hard of Hearing	6.08	5.80	5.92	4.89	4.66
Department of Accounts	6.38	6.36	6.02	5.33	6.07
Department of Aviation	7.00	7.00	6.71	7.00	7.00
Department of Behavioral Health and Development Services	5.87	4.65	5.30	4.22	4.91
Department of Conservation and Recreation	6.53	6.63	6.63	5.50	6.04
Department of Corrections	3.04	3.22	3.06	3.00	3.00
Department of Criminal Justice Services	3.93	1.80	2.02	1.67	1.54
Department of Education	0.00	0.00	0.00	0.00	0.00
Department of Elections	5.83	5.80	5.77	6.00	5.55
Department of Environmental Quality	3.32	3.26	3.57	4.44	2.97
Department of Fire Programs	0.00	0.00	0.00	0.00	0.00
Department of Forensic Science	5.08	5.40	5.66	4.67	5.04
Department of Forestry	0.00	0.00	0.00	0.00	0.00
Department of Game and Inland Fisheries	0.00	0.00	0.00	0.00	0.00
Department of General Services	0.00	0.00	0.00	0.00	0.00
Department of Health	0.00	0.00	0.00	0.00	0.00

Agency Name	Detect	Identify	Protect	Recover	Respond
Professions					
Department of Historic Resources	5.87	5.76	5.36	5.78	4.69
Department of Housing and Community Development	0.00	0.00	0.00	0.00	0.00
Department of Human Resource Management	5.89	5.76	5.62	5.67	5.81
Department of Juvenile Justice	6.08	6.10	6.25	6.00	6.00
Department of Labor and Industry	5.53	5.48	5.85	6.00	5.52
Department of Medical Assistance Services	0.00	0.00	0.00	0.00	0.00
Department of Military Affairs	0.00	0.00	0.00	0.00	0.00
Department of Mines, Minerals and Energy	5.28	3.88	5.67	5.11	5.59
Department of Motor Vehicles	5.28	6.24	5.89	5.33	6.47
Department of Planning and Budget	5.78	5.55	5.97	5.61	5.96
Department of Professional and Occupational Regulation	0.00	0.00	0.00	0.00	0.00
Department of Rail and Public Transportation	0.00	0.00	0.00	0.00	0.00
Department of Small Business and Supplier Diversity	5.89	5.77	5.68	5.67	5.68
Department of Social Services	0.00	0.00	0.00	0.00	0.00
Department of Taxation	0.00	0.00	0.00	0.00	0.00
Department of Treasury	6.00	5.60	6.05	5.56	6.00
Department of Veterans Services	0.00	0.00	0.00	0.00	0.00
Frontier Culture Museum of Virginia	5.69	5.57	5.62	5.83	5.43
Gunston Hall	5.57	5.87	5.73	5.33	5.39
Indigent Defense Commission	0.00	0.00	0.00	0.00	0.00
Jamestown-Yorktown Foundation	0.00	0.00	0.00	0.00	0.00
Library of Virginia	0.00	5.25	5.72	0.00	0.00
Marine Resources Commission	5.87	5.35	5.48	4.94	5.09
Motor Vehicle Dealer Board	0.00	0.00	0.00	0.00	0.00
Norfolk State University	0.00	0.00	0.00	0.00	0.00
Office for Children's Services	0.00	0.00	0.00	0.00	0.00
Office of Attorney General	0.00	0.00	0.00	0.00	0.00
Office of State Inspector General	2.60	7.00	5.62	7.00	5.30
Office of the Governor	5.93	5.76	5.82	6.00	5.72
Richard Bland College	0.00	0.00	0.00	0.00	0.00
Science Museum of Virginia	0.00	0.00	0.00	0.00	0.00
Southern Virginia Higher	5.87	5.86	5.82	5.33	5.59

Agency Name	Detect	Identify	Protect	Recover	Respond
Education Center					
State Corporation Commission	0.00	0.00	0.00	0.00	0.00
State Council of Higher Education for Virginia	0.00	0.00	0.00	0.00	0.00
State Lottery Department	0.00	0.00	0.00	0.00	0.00
Tobacco Region Revitalization Commission	0.00	0.00	0.00	0.00	0.00
Virginia College Savings Plan	0.00	0.00	0.00	0.00	0.00
Virginia Commission for the Arts	0.00	0.00	0.00	0.00	0.00
Virginia Department of Agriculture and Consumer Services	2.39	5.25	5.66	5.22	2.91
Virginia Department of Emergency Management	3.87	4.04	4.03	6.00	5.52
Virginia Department of Health	5.10	5.50	5.21	1.00	2.60
Virginia Department of Transportation	3.60	3.70	4.05	3.33	2.54
Virginia Economic Development Partnership	0.00	0.00	0.00	0.00	0.00
Virginia Employment Commission	0.00	0.00	0.00	0.00	0.00
Virginia Foundation for Healthy Youth	0.00	0.00	0.00	0.00	0.00
Virginia Information Technologies Agency	7.00	6.33	6.70	6.72	6.96
Virginia Information Technologies Agency	6.04	6.04	6.26	6.17	6.35
Virginia Museum of Fine Arts	5.47	5.50	5.75	5.33	5.35
Virginia Museum of Natural History	5.38	5.37	5.60	5.00	5.43
Virginia Racing Commission	0.00	0.00	0.00	0.00	0.00
Virginia Resources Authority	0.00	0.00	0.00	0.00	0.00
Virginia Retirement System	0.00	0.00	0.00	0.00	0.00
Virginia School for the Deaf and Blind	0.00	0.00	0.00	0.00	0.00
Virginia State Police	0.00	0.00	0.00	0.00	0.00
Virginia State University	0.00	0.00	0.00	0.00	0.00
Virginia Workers Compensation Commission	6.06	7.00	6.51	5.22	6.29